VYSOKÁ ŠKOLA BÁŇSKÁ – TECHNICKÁ UNIVERZITA OSTRAVA
EKONOMICKÁ FAKULTA

DIPLOMOVÁ PRÁCE

2010 Bc. Marian Pieczka

VYSOKÁ ŠKOLA BÁŇSKÁ – TECHNICKÁ UNIVERZITA OSTRAVA
EKONOMICKÁ FAKULTA

KATEDRA APLIKOVANÉ INFORMATIKY

Racionalizace počítačové sítě lázní

The Rationalization of the Computer Network of Spa

Student: Bc. Marian Pieczka

Vedoucí diplomové práce: Ing. Petr Rozehnal, Ph.D.

Ostrava 2010

VŠB-Technická univerzita Ostrava | Ekonomická fakulta
Katedra: Aplikovaná informatika | Akademický rok 2009/2010

ZADÁNÍ DIPLOMOVÉ PRÁCE

Řešitel:	Bc. Marian Pieczka
Program:	Systémové inženýrství a informatika
Obor:	Aplikovaná informatika
Téma:	Racionalizace počítačové sítě lázní
	The Rationalization of the Computer Network of Spa

1. Úvod
2. Teoretická východiska, vymezení pojmů
3. Analýza současného stavu
4. Návrh racionalizace počítačové sítě
5. Zhodnocení přínosu navrhovaného řešení
6. Závěr

Seznam použité literatury
Seznam zkratek
Prohlášení o využití výsledků diplomové práce
Přílohy

Odborná literatura:

TKULOVE, James. *Sítě LAN : Hardware, instalace, zapojení*. Tomáš Znamenáček. 1. vyd. Brno : Grada Publishing, 2009. 384 s. ISBN 978-80-247-2098-2.
WILLIAMS, Andrew. *Firewall policies and VPN Configurations*. Canada : Syngress Publishing, 2006. 482 s. ISBN 1-59749-088-1.
LUHOVÝ, Karel. Virtuální privátní sítě VPN. *Svět sítí* [online]. 6. ledna 2003, 6, [cit. 2010-03-10]. Dostupný z WWW: <www.svetsiti.cz>.

Vedoucí:	Ing. Petr Rozehnal, Ph.D.
Datum zadání:	20. listopadu 2009
Datum odevzdání:	30. dubna 2010

Ing. Jan Ministr, Ph.D	prof. Dr. Ing. Dana Dluhošová
vedoucí katedry	*děkanka fakulty*

Místopřísežně prohlašuji, že jsem celou práci včetně všech příloh vypracoval samostatně.

V Ostravě dne

Na tomto místě bych využil příležitost k poděkování IT manažerovi za spolupráci a poskytnuté informace a rovněž mému vedoucímu diplomové práce panu Ing. Petru Rozehnalovi, Ph.D. za vedení a konzultace v průběhu psaní práce.

OBSAH

1 Úvod 1

2 Teoretická východiska, vymezení pojmů 3
2.1 Pojem počítačová síť 3
2.1.1 Lokální počítačová síť (LAN – Local Area Network). 3
2.1.2 Rozlehlá počítačová síť (WAN – Wide Area Network). 3
2.2 Pojem virtuální privátní síť 4
2.2.1 Zapouzdření IP 5
2.2.2 Šifrovaná autentizace 6
2.2.2.1 Šifrování pomocí tajného klíče 7
2.2.2.2 Šifrování na principu veřejného klíče 7
2.2.3 Šifrování datové částí 8
2.3 Typy VPN 8
2.3.1 VPN založené na serverech 8
2.3.2 VPN založené na firewallech 10
2.3.3 VPN založené na směrovačích 11
2.4 Architektury VPN 11
2.4.1 VPN s okruhy 11
2.4.2 Hvězdicovitá VPN 13
2.4.3 Hybridní VPN 14
2.5 Typologie sítí VPN 15
2.5.1 VPN na síťové vrstvě 16
2.5.1.1 Filtrování směrovacích informací 16
2.5.1.2 VPN založené na tunelování 16
2.5.2 VPN na spojové vrstvě 17
2.6 Běžné implementace VPN 18
2.6.1 IPSec 19
2.6.2 PPTP 20
2.6.3 Protokol pro režim tunel na vrstvě 2 (L2TP) 21
2.6.4 PPP/SSL nebo PPP/SSH 21
2.7 Bezpečný vzdálený přístup 22
2.7.1 VPN u ISP 22
2.7.2 VPN v klientském počítači s vytáčeným připojením 23

3 Analýza současného stavu 25
3.1 Objekt řešení 25
3.1.1 O firmě Lázně Darkov, a.s. 25
3.1.1.1 Léčebna darkov 26
3.1.1.2 Rehabilitační sanatorium 26
3.2 Firemní počítačová síť, současný stav 27
3.2.1 Hardwarové vybavení sítě 27
3.2.1.1 Hardwarový firewall 27
3.2.1.2 Hlavní směrovač (router) 28
3.2.1.3 Demilitarizovaná zóna 29
3.2.1.4 Server 30
3.2.1.5 Sítě LAN 30
3.2.1.6 Síť WAN 31
3.2.2 Připojení k Internetu 31

3.2.3 Zhodnocení analýzy 31

4 Návrh racionalizace počítačové sítě 32
4.1 Hardwarové řešení propojení pracovišť Rehabilitačního sanatoria a Léčebny Darkov. 33
4.1.1 Hardwarové VPN 34
4.1.2 Návrh variant 35
4.1.2.1 Výběr nejlepší varianty a cenová kalkulace 35
4.1.3 WAN vs. VPN 36
4.1.2.1 VPN jsou levnější než WAN 36
4.1.2.2 Snadnější implementace VPN 37
4.1.2.3 VPN jsou pomalejší než WAN 38
4.1.2.4 VPN jsou méně spolehlivé oproti WAN. 39
4.1.2.5 VPN jsou méně bezpečné než izolované LAN nebo WAN. 39
4.2 Softwarové řešení vzdáleného přístupu 40
4.2.1 Softwarové VPN 40
4.2.2 Návrh variant 41
4.2.2.1 První kolo výběru nejlepší varianty 45
4.2.2.2 Výběr nejlepší varianty a cenová kalkulace 45
4.3 Přednosti a limity VPN u vzdáleného přístupu 46
4.3.1 Přínosy a přednosti 46
4.3.2 Limity VPN 47
4.4 Softwarové vs. Hardwarové řešení 48

5 Zhodnocení přínosu navrhovaného řešení 50
5.1 Zhodnocení přínosu změny pronajaté linky na VPN spojení 50
5.1.1 Kvantitativní zhodnocení 50
5.1.2 Kvalitativní zhodnocení 51
5.2 Zhodnocení přínosu vzdáleného přístupu pomocí VPN 52
5.2.1 Kvantitativní zhodnocení 52
5.2.2 Kvalitativní zhodnocení 52

6 Závěr 53

Seznam použité literatury 54

Seznam zkratek a symbolů 56

Prohlášení o využití výsledků diplomové práce 57

1 ÚVOD

V mé diplomové práci se zabývám racionalizací počítačové sítě lázní.

Základní motivace pro budování virtuálních privátních sítí leží v ekonomice. Dnešní komunikační systémy se vyznačují vysokými fixními náklady a relativně nízkými variabilními náklady, závislými na přenosové kapacitě či šířce pásma. V takovémto ekonomickém prostředí je pak finančně výhodné spojit větší počet diskrétních komunikačních služeb do společné výkonné platformy a "rozpustit" tak vysoké pevné náklady mezi velký počet klientů. V duchu této myšlenky je pak vybudování i provoz celé sady virtuálních sítí na společné fyzické komunikační základně levnější než vybudování a provoz fyzicky samostatných diskrétních sítí.

Pro budování VPN existuje několik důvodů, jejich společným jmenovatelem je požadavek "virtualizace" jisté části komunikace v dané organizaci. Řečeno jinými slovy, požadavek "skrýt" jistou část komunikace (možná i celou) před "ostatním světem" a přitom využít efektivity společné komunikační infrastruktury, nejčastěji Internetu.

Hlavním impulsem rozvoje VPN je mohutný rozvoj Internetu. Internet, se svojí prakticky celosvětovou dostupností umožňuje snadnou výměnu dat mezi libovolnými připojenými uzly na světě. Internet je vybudován na jednotném adresovém schématu a směrovací hierarchii, všechny připojené entity sdílejí společnou síťovou infrastrukturu. Dokud byly firemní pobočky propojeny pevnými linkami nebo frame - relay spoji od zpravidla státního telekomu (tzv. plně privátní sítě), nikdo necítil zvláštní potřebu chránit svá data. Situace se ale výrazně změnila, když vznikla možnost a nabídka levného propojení poboček (nebo připojení uživatele k centrále) přes Internet. Ve své podstatě pak velice podobný problém představuje bezpečné připojení uživatelů na WWW server. Používají se zde podobné techniky virtualizace s tím rozdílem, že zde zpravidla není dopředu jasné, kteří uživatelé se budou připojovat.

Spojování jednotlivých komunikačních služeb do jedné společné a veřejné platformy má ale své limity, a těmi jsou právě výše zmíněné požadavky na "privátnost" komunikace - požadavky na vzájemné "odstínění" komunikace mezi jednotlivými uživateli či skupinami uživatelů. Náročnost řešení tohoto vzájemného odstínění je pak úměrná výši požadavků na bezpečnost a integritu dat jednotlivých komunikujících klientů či skupin.

Cílem mé diplomové práce je navrhnout možnosti využití virtuálních privátních sítí v lázních a zhodnotit jeho přínos pro firmu a její zaměstnance a vytvořit tak podklad pro rozhodnutí, zda ve firemní síti VPN využívat.

2 TEORETICKÁ VÝCHODISKA, VYMEZENÍ POJMŮ

2.1 POJEM POČÍTAČOVÁ SÍŤ

Pod pojmem počítačová síť si snad každý dokáže představit soustavu vzájemně propojených počítačů .

2.1.1 Lokální počítačová síť (LAN – Local Area Network).

Sítě LAN označují všechny malé sítě, které si mnohdy vytváří sami uživatelé na své vlastní náklady(viz lit. [16]). Jedná se o sítě uvnitř místností, budov nebo malých areálů; ve firmách i v domácnostech. Dále je charakterizuje levná vysoká přenosová rychlost (až desítky Gbps) a skutečnost, že si je na vlastní náklady pořizují sami majitelé propojených počítačů.

Slouží ke snadnému sdílení prostředků, které jsou v LAN dostupné. Nejvyšší podíl při komunikaci v LAN má obvykle sdílení diskového prostoru. Dále LAN umožňuje využívat tiskáren, které jsou připojeny k jiným počítačům nebo vystupují v síti samostatně, sdílet připojení k Internetu a dalších k němu návazných služeb (WWW, E-mail, Peer-to-peer sítě a podobně).

2.1.2 Rozlehlá počítačová síť (WAN – Wide Area Network).

WAN je počítačová síť, která pokrývá rozlehlé geografické území (například síť, která překračuje hranice města, regionu nebo státu) (viz lit. [16]). Největším a nejznámějším příkladem sítě WAN je síť Internet.

Sítě WAN jsou využívány pro spojení lokálních sítí (LAN) nebo dalších typů sítí, takže uživatelé z jednoho místa mohou komunikovat s uživateli a počítači na místě jiném. Spousta WAN je budována pro jednotlivé společnosti a jsou soukromé. Ostatní, budované poskytovateli připojení, poskytují služby pro připojení sítí LAN do Internetu. Sítě WAN bývají budovány na pronajatých linkách (leased lines). Tyto linky často bývají velmi drahé.

Častěji se sítě WAN budují na metodách přepojování okruhů (circuit switching) nebo přepojování paketů (packet switching). Síťové služby používají pro přenos a adresaci protokol TCP/IP. Poskytovatelé služeb připojení častěji používají pro přenos v sítích WAN protokoly ATM a Frame Relay. Protokol X.25 byl užíván v raných počátcích sítí WAN a bývá označován jako 'praotec' protokolu Frame Relay.

V dnešní době se tyto dvě počítačové sítě LAN a WAN rozdělují spíše intuitivním způsobem.

2.2 POJEM VIRTUÁLNÍ PRIVÁTNÍ SÍŤ

Co je to **virtuální privátní síť, VPN (Virtual Private Network)**? Stejně jako se to v počítačovém průmyslu stává docela často, i zde pokřik nabubřelého marketingu zastírá jinak docela jasný význam. V případě sítí VPN panuje určitá nejasnost ohledně toho, co je vlastně na síti VPN *virtuální* – je to ono soukromí (privátnost), anebo síť? Tyto dva body podávají definici virtuální privátní sítě: [5]

- Topologie virtuální privátní sítě VPN je provozována převážně nad *sdílenou* síťovou infrastrukturou, obvykle nad běžným, veřejným Internetem, přičemž v každém z koncových bodů se nachází alespoň jeden privátní segment sítě LAN.
- Relace sítě VPN běží nad šifrovaným spojením.

Aby mohly síťové segmenty na jednotlivých koncích sítě VPN správně pracovat nad šifrovaným spojením po veřejném Internetu, musí podléhat administrativní kontrole stejného podniku (nebo podniků), jenž danou virtuální síť provozuje. Prakticky vzato to znamená, že koncové směrovače sítě VPN musí podléhat společné bezpečnostní a provozní správě; tyto směrovače v koncových bodech virtuální sítě VPN musí především pracovat s jedním společným schématem šifrování. [5]

Připojení k internetovým sítím na velkou vzdálenost se klasicky zajišťovala pomocí sítě WAN s pronajatou pevnou linkou. Pro člověka, který je často na cestách a na žádném místě se nezdržuje tak často, aby se mu pevná linka vyplatila, je ovšem toto řešení nereálné. Virtuální privátní sítě dnes zásadním způsobem ovlivňují trh pronajatých linek zejména z následujících důvodů: [5]

- **Nižší náklady.** Pronajaté linky vyžadují ke své činnosti drahé vybavení pro potřebnou přenosovou šířku pásma a pro páteřní síť. Navíc, virtuální sítě VPN nepotřebují na koncové straně žádný zvláštní terminál ani přístupové modemy.

- **Přizpůsobivost virtuální sítě.** Linky virtuálních privátních sítí se dají relativně snadno a za levné peníze vytvořit, změnit nebo odstranit. Komunikační infrastruktura dané organizace není tudíž při instalaci, změně konfigurace ani odstranění sítě VPN nijak vážně zasažena. Díky široké dostupnosti Internetu se kromě toho do virtuální privátní sítě snadno dostaneme prakticky odkudkoli.
- **Snadný přístup.** Vzhledem k dobré dostupnosti mají účastníci sítě VPN v libovolném jejím místě k dispozici stejnou úroveň přístupu k centrálním službám, které jsou navíc pro ně ve stejné podobě (jako například elektronická pošta, interní a externí webové servery, bezpečnost atd.).

Virtuální privátní sítě řeší problém přímého přístupu přes Internet na servery kombinací těchto základních prvků zabezpečení (viz lit. [3]):

- Zapouzdření IP
- Šifrovaná autentizace
- Šifrování datové částí

V pravé VPN musí být přítomny všechny tři prvky. Ačkoliv se na první pohled může zdát, že šifrovaná autentizace a šifrování datové části jsou to samé, ve skutečnosti se jedná o zcela odlišné funkce a mohou existovat nezávisle na sobě. Například SSL (Secure socket layer) provádí šifrování datové části bez šifrované autentizace vzdáleného uživatele a standardní přihlašování ve Windows provádí zase šifrovanou autentizaci, aniž by šifrovalo datové části. [3]

2.2.1 Zapouzdření IP

Při propojování samostatných sítí LAN přes Internet je nutné najít způsob, jak chránit datový provoz, který mezi těmito sítěmi LAN prochází. V ideálním případě by neměly počítače v jednotlivých sítích LAN vědět, že na komunikaci s počítači v jiné síti LAN je něco zvláštního. Počítače vně virtuální sítě by neměly mít možnost zachytávat provoz, který se vyměňuje mezi jednotlivými sítěmi LAN, či vkládat do komunikačního toku svá vlastní data. V podstatě je zapotřebí privátní a chráněný tunel přes veřejný Internet.

Paket IP může obsahovat jakýkoliv druh informací: programové soubory, údaje z tabulkového procesoru, zvukové toky anebo i jiné pakety IP. Jakmile paket IP obsahuje jiný paket IP, říká se tomuto typu vkládání zapouzdření IP, IP přes IP nebo IP/IP.

IP se zapouzdřuje z důvodu kontaktování hostitelského počítače v jiné síti, když není možné ustavit přímé síťové připojení. Zapouzdřením IP vznikne u síťových počítačů představa, že dvě vzdálené sítě jsou vlastně sítě sousedící – oddělené pouze jedním směrovačem. Ale ve skutečnosti je dělí mnoho internetových směrovačů a bran, které nemusí ani používat stejný adresový prostor, protože obě interní sítě překládají adresy.

Zapouzdření IP také umožňuje kontaktovat vzdálený hostitelský počítač v rezervovaných blocích 10 a 192.168, které nejsou jinak přes Internet směrovatelné. Když se přidělovaly rezervované bloky sítě 10.0.0.0/8 a 192.168.0.0/16, byla vytvořena pravidla směrování. Zajišťovala, že tyto bloky nebylo možné směrovat přes Internetovou páteřní síť, aby bylo možno poskytnout trochu zabezpečení a zamezit konfliktům s dalšími sítěmi, které používaly stejný blok adres. Nikdo nemohl přes Internet hostitelské počítače v uvedeném síťovém intervalu kontaktovat, takže pokud jste tyto intervaly použili v privátní síti, byli jste před hackerskými útoky relativně v bezpečí a adresový prostor sítě nekolidoval s veřejnými adresami někoho jiného. Tato pravidla stále platí a relativně dobře svůj účel plní, ale pokud chcete propojit vzdálená pracoviště a používat rezervované bloky adres, musíte je zapouzdřit do paketů IP, které lze směrovat přes veřejný Internet.

Koncový bod tunelu - ať už se jedná o směrovač, zařízení VPN nebo server, na němž je protokol pro tvorbu tunelů - bude přijímat veřejné pakety IP, odstraní z nich interní paket, dešifruje ho (pokud je zašifrovaný - nemusí tomu tak být) a pak na něj uplatní svoje pravidla směrování a pošle vložený paket po určené trase na privátní síť.

2.2.2 Šifrovaná autentizace

Šifrovaná autentizace se používá na bezpečné ověření totožnosti vzdáleného uživatele, aby systém mohl určit, jaká úroveň zabezpečení je pro uvedeného uživatele přiměřena. VPN pomocí šifrované autentizace určují, zda se může uživatel účastnit šifrovaného tunelu či nikoliv a mohou také autentizaci použít k výměně tajných nebo veřejných klíčů pro šifrování datové části.

Šifrovaná autentizace má dva druhy: šifrování pomocí tajného klíče a šifrování na principu veřejného klíče.

2.2.2.1 Šifrování pomocí tajného klíče

Také se mu říká šifrování pomocí sdíleného tajemství, spoléhá se na tajnou hodnotu, kterou znají obě strany. Prostá znalost hodnoty dokládá tomu, kdo klíč poskytuje, že žadatel o klíč je důvěryhodný. Pomocí komunikace typu výzva a odezva lze zjistit, že se po síti přenáší pouze hodnota hash tajemství, nikoliv samotné tajemství. Variacemi jednorázových hesel (one - time password) lze zase zajistit, že tajemství se po každém použití mění.

Problém se šifrováním pomocí tajného klíče spočívá ve výměně klíčů. Neexistuje žádný skutečně bezpečný způsob, jak by se mohly obě strany najednou tajný klíč „dozvědět“, aniž by proběhla předtím nějaká forma nezašifrované komunikace. Obvykle k výměně dochází v mysli jedince, který nastaví na dvou různých koncových systémech stejný tajný klíč.

Algoritmy šifrování na principu tajného klíče jsou mnohonásobně (alespoň tři z nich) rychlejší než algoritmy šifrování na principu veřejného klíče. Ve většině implementovaných systémů se bezpečná autentizace provádí šifrováním na principu veřejných klíčů a ustavením komunikačního kanálu a uvedeným kanálem se pak bezpečně vymění sada tajných klíčů, takže lze použít vysokorychlostní algoritmus šifrování tajným klíčem.

2.2.2.2 Šifrování na principu veřejného klíče

Spoléhá se na výměnu jednosměrných klíčů - klíčů, které lze použít pouze k zašifrování nebo dešifrování dat, ale nikoliv obojího. Klíč k dešifrování (privátní klíč) je uložen pouze na systému příjemce a nikdy se nepřenáší přes veřejnou síť. To zašifrovaná data během jejich přenosu přes veřejnou síť zabezpečuje, protože je nikdo jiný nemůže dešifrovat, i kdyby měl k dispozici šifrovací klíč (veřejný klíč). Koncové systémy tunelu si mohou vyměňovat dvojice veřejných klíčů, čímž vytvoří obousměrný kanál. Nebo příjemce veřejného klíče může zašifrovat sdílený tajný klíč a poslat ho na systém, který vyslal veřejný klíč, a pak ho použít pro budoucí komunikace (protože šifrováni pomocí tajného klíče -
- symetrická šifra je rychlejší než šifrování pomocí veřejných klíčů - asymetrická šifra).

Pokud by hacker zachytil veřejný nebo šifrovací klíč, může data pouze šifrovat a přenášet je příjemci. Není však schopen obsah dat, který zachytí, dešifrovat.

2.2.3 Šifrování datové částí

Šifrování datové části se používá k zamlžení obsahu vložených dat, aniž by bylo nutné celý paket zapouzdřovat do jiného paketu. V tom je šifrování datové části stejné jako standardní propojování sítí IP, kromě toho, že datová část se šifruje. Šifrování datové části data zamlží, ale neutajuje informace hlavičky, takže z nich lze zjistit podrobnosti o interní síti.

Šifrování datové části lze doplnit jednou z řady bezpečných šifrovacích technik, které se liší podle zvoleného řešení VPN.

2.3 TYPY VPN

Nejjednodušší příklad připojení k VPN se směrováním je připojení prostřednictvím IPSec, protože neobsahuje běžné prvky zabezpečení Internetu jako jsou firewally a proxy servery. Představuje ale jeden typ VPN: VPN založenou na směrovačích. Mnoho firewallů také obsahuje funkce vytváření tunelů IP, na nichž může být založena VPN. Střední až velké sítě používají směrovače ke správě provozu, který se směruje v síti LAN, z ní i do ní. Existuje i mnoho směrovačů pouze pro VPN. Těmto směrovačům se říká zařízení VPN, protože plní pouze jednu funkci. Bez ohledu na to, jak je VPN nastavena, každá řádně zabezpečená síť s připojením k Internetu bude obsahovat firewall a potenciálně i služby proxy serveru. VPN je nutné nakonfigurovat, aby s těmito službami spolupracovala. [3]

Existují 3 typy VPN:

- VPN založené na serverech
- VPN založené na firewallech
- VPN založené na směrovačích, včetně zařízení VPN

2.3.1 VPN založené na serverech

V síti založené na Windows je snad nejjednodušším a nejméně destruktivním způsobem propojení jednotlivých sítí LAN pomocí VPN vyhradit pro směrování provozu VPN samostatný server. Stávající služby firewallu, směrovače a serveru proxy lze ponechat na místě a jediná požadovaná úprava nastavení zabezpečení Internetu spočívá v tom, že firewall bude propouštět šifrované porty přes server Windows s RRAS (Routing and Remote

Access Service). Windows NT podporovaly pouze PPTP, ale Windows 2000 a novější podporují PPTP, L2TP i IPSec. [3]

Díky Linuxu a *open - source* komunitě byly zavedeny do světa Unixu silné nástroje na zabezpečení, např. Blowfish, Free S/WAN, a PPP přes SSL a podpora pro PPTP a L2TP. Mnoho dodavatelů Unixu začleňuje IPSec i do svých implementací TCP/IP. Pomocí všech uvedených produktů lze mezi sítěmi LAN vytvořit VPN s využitím běžných počítačů.

Přestože jsou Windows 2000 plně hodnotný operační systém, na kterém může být provozován současně firewall, zašifrovaná propojení pomocí mnoha protokolů a služby sdílení souborů a tiskáren klientským počítačům v síti, není dobré provozovat toto vše pouze na jednom počítači. Selhání zabezpečení v jedné z těchto služeb může oslabit celou síť a nikoliv jenom napadený počítač. Server RRAS například nemusí být v síti privilegovaný počítač. Musí jenom zapouzdřovat a z pouzder vyjímat síťový provoz. Hacker, který napadne řádně izolovaný server RRAS, bude muset stejně překonat standardní zabezpečení sítě LAN (uživatelská jména a hesla) a bude muset přejít přes firewall, aby se k serveru RRAS dostal. Pokud služby RRAS poskytuje i souborový server, hacker by měl přístup okamžitě ke všem souborům v síti. [3]

Je dobré vědět, že provoz VPN, který je určen vzdálené síti na VPN, prochází stejnou sítí LAN vždy dvakrát - jednou ve formě běžného provozu LAN na server RRAS a pak znovu v zapouzdřené podobě ze serveru RRAS na firewall. I když zdvojení provozu v LAN je nevýhodné, objem provozu je obvykle v porovnání s běžným provozem na LAN nevýznamný, protože přenosová kapacita připojení k Internetu omezuje objem informací, které lze přes zašifrované propojení poslat.

Server Windows 2000 se dodává se vším, co je zapotřebí k ustavení virtuální privátní sítě přes Internet pomocí PPTP, L2TP nebo IPSec. Ale implementace PPTP ve Windows 2000 je závadná a měla by se považovat za bezpečnou pouze do určité míry. Pokud budeme VPN stavět s využitím Windows 2000, nejlepším možným zabezpečením je použití IPSec. Možná bude zapotřebí i další software, aby se síť mohla chránit před vniknutím přes IP, i když k ustavení bezpečného zašifrovaného připojení bezpečných sítí LAN stačí služba RRAS, která se dodává s operačním systémem. [3]

Spojením funkcí Maskování IP a IP Chains (Masquerade IP/IP Chains) v Linuxu a dalšího softwaru *open - source* lze vytvořit poměrně solidní VPN. Ale správná integrace programů od různých dodavatelů není jednoduchá a může vést v zabezpečení k efektu „ementálu“. Všechny prvky jsou nainstalované, ale mezi těmito prvky existují průchody, protože integrace nebyla provedena správně.

2.3.2 VPN založené na firewallech

Všechny sítě LAN, které jsou připojeny k Internetu, potřebují firewall, aby oddělily provoz LAN (provoz NetBios v případě sítí NT; v případě sítí na Unixu provoz NFS, Telnet nebo X-Windows; v případě sítí založených na systému Macintosh pak provoz AppleTalk a v případě zděděných sítí NetWare provoz NCP) id Internetového provozu. Firewall by měl blokovat přístup ke všem portům, které se výslovně nepožádají k poskytování služeb – zvláště k portům NetBIOS, NFS, Telnet nebo X-Windows – z umístění mimo síť a měl by specifikovat, které počítače v síti mají přístup na Internet povolen. [3]

To však nevyčerpává všechny možnosti moderních firewallů. Některé populární firewally umí provádět překládání adres. Mohou se starat o filtrování protokolů a portů. Mohou přesměrovávat běžné služby jako je pošta, news a FTP, a mohou dokonce zprostředkovávat přes proxy protokoly jako HTTP, SMTP, NNTP, Telnet, a FTP. Protože firewally už provádějí u síťových paketů všechny možné druhy analýz a transformací, je jednoduché do firewallu začlenit i funkci vytváření tunelů IP.

Původně byly protokoly pro tunely, které byly začleněny ve většině firewallů prioprietární a propojení na VPN se s nimi mohlo ustavovat pouze ve spojení se stejnou značkou firewallu na vzdálené síti LAN nebo s klientským softwarem, jenž byl vytvořen speciálně pro uvedený firewall. S všeobecným zaváděním šifrovacích a dohadovacích protokolů typu IPSec+IKE (*IP Security + Internet Key Exchange*) se situace nyní výrazně mění. Ikdyž mnoho dodavatelů nyní IPSec+IKE podporuje i v sítích s více dodavateli, je vhodné se na jednotlivé dodavatele obrátit a dotázat se, zda svůj software přezkoušeli, aby fungoval s ostatními firewally v síti. Také je dobré vyjasnit si veškeré otázky ohledně konfigurace. Zcela standardizovaná implementace IPSec+IKE by měla vylučovat problémy s kompatibilitou, které způsobují šifrovací systémy vlastněné jednou společností. [3]

Většina firewallů obsahuje software VPN, kterým se jednotlivé vzdálené klientské počítače připojují k firewallům a ustavují tunel. Pokud se k síti LAN připojují vzdálené počítače, je nutné zkontrolovat, zda je klientský software k dispozici pro všechny podporované platformy. Pak se také musí nainstalovat program s funkcemi firewallu na jednotlivých počítačích, a to k zabezpečení jinak nechráněných počítačů před napadením, když se připojují k síti VPN.

2.3.3 VPN založené na směrovačích

Velké sítě (např. podnikové, školní, vládní nebo univerzitní sítě) často sestávají z několika segmentů LAN propojených směrovači. Směrovače izolují provoz na interních segmentech LAN a přenášejí rychle a výkonně provoz mezi jednotlivými sítěmi LAN. Směrovače jsou zvláštní hardwarová zařízení se specializovanou elektronikou a programováním a používají se k manipulaci se síťovými pakety. [3]

Jednoduché směrovače pouze přenášejí síťové pakety z jednoho segmentu na jiný, ale složitější a dražší směrovače mohou fungovat i jako firewally, přičemž síťový provoz zkoumají a zpracovávají (blokují porty, mění směrování paketů atd.) podle pravidel, která stanoví síťový administrátor. Některé směrovače dokonce obsahují funkci zapouzdřování síťového provozu a ustavování propojení přes VPN mezi směrovači. Mezi tři oblíbená řešení pro směrovače, které podporují funkce VPN, patří rodina směrovačů 2210 od IBM, směrovače Cisco s IOS a přepínače MAX od firmy Ascend.

2.4 ARCHITEKTURY VPN

Podle počtu účastníků ve VPN existují tři základní konfigurace VPN (viz lit. [3]):

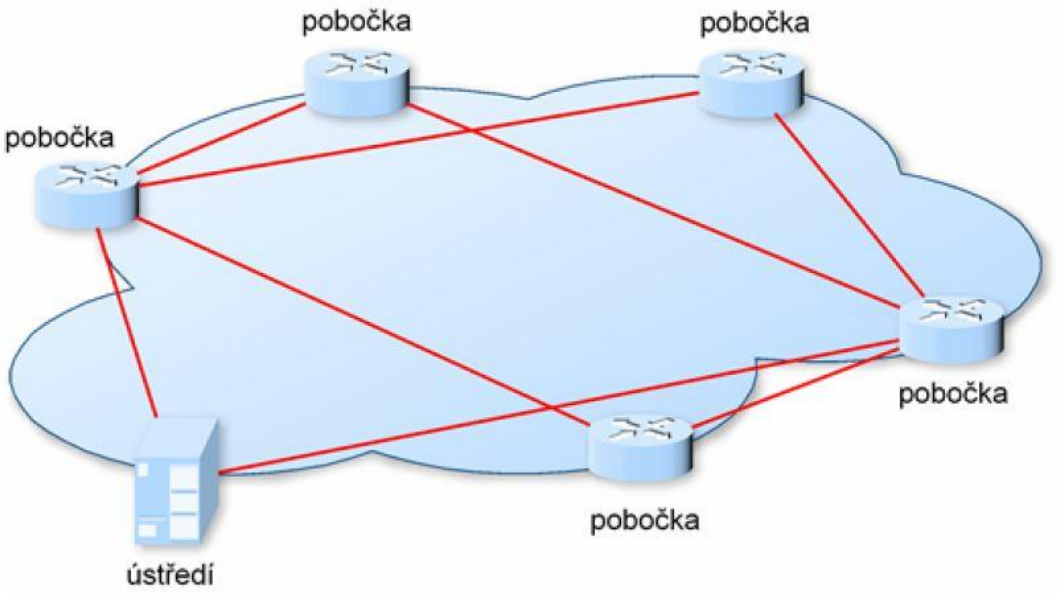
- Síť s okruhy, kde má každý účastník přímou bezpečnostní asociaci s každým dalším účastníkem.
- Rozbočovač a paprsky (také se jí říká síť do hvězdice), kde má každý účastník jednu bezpečnostní asociaci na ústřední směrovač VPN, který má bezpečnostní asociaci z každým zařízením VPN.
- Hybridní VPN, tj. kombinace dvou výše uvedených architektur, přičemž se jedná buď o síť s okruhy s rozbočovači anebo o hvězdici s rozbočovači.

Z těchto dvou je síť s okruhy výkonnější a hvězdice je spolehlivější.

2.4.1 VPN s okruhy

VPN s okruhy vytvářejí konkrétní propojení mezi každými dvěma účastníky v síti VPN. To vyžaduje, aby v každém zařízení v síti VPN byla k dispozici SA (security association – bezpečnostní asociace) - neboli definice VPN. Jednodušší kompromis

představuje částečná typologie VPN s okruhy, kdy nejsou všechny uzly přímo navzájem propojeny. Tato typologie je na obrázku 2.4.1-1.



Obr. 2.4.1-1 VPN s okruhy

Když chce zařízení VPN vyslat data, podívá se do své směrovací/SA tabulky a určí, které propojení VPN by mělo být k přenosu dat použito. Data se pak pošlou přímo přes Internet na vzdálený koncový bod VPN.

Vytvoření velké VPN s okruhy může být problematické, protože jednotlivé SA vyžadují paměťovou kapacitu na všech zařízeních, což znamená, že i ta nejmenší zařízení v síti musí mít dostatečnou kapacitu paměti flash pro celou sadu zařízení ve VPN. Pro většinu uživatelů to není až tak palčivý problém, protože moderní zařízení mají dost kapacity na zpracovávání více připojení.

Větším problémem u VPN s okruhy je požadavek, aby každé zařízení VPN na síti WAN bylo aktualizováno pokaždé, když se přidá nový koncový bod VPN, k čemuž v rozšiřující se síti může docházet relativně často. Pokud se síť k počítačům se vzdálenými uživateli chová jako k plnohodnotným účastníkům, může být tato otázka skutečně velmi problematická.

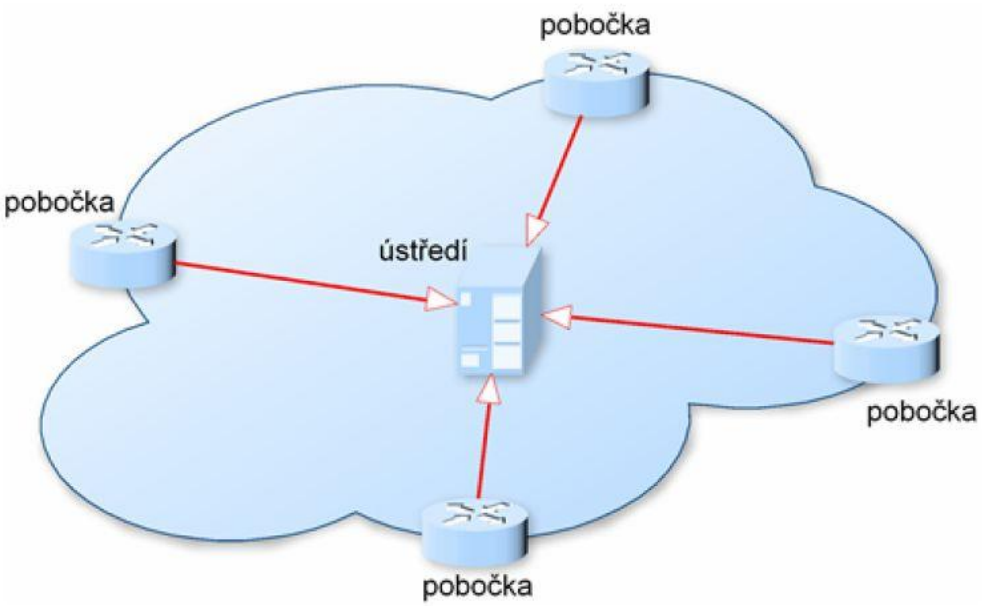
Vzdálené aktualizace VPN jsou problematické samy o sobě, protože údaje o aktualizaci se musí přenášet přes stávající VPN a pak musí být zařízení odpojeno, provedena aktualizace a zařízení znovu připojeno k VPN. V případě, že dojde k problému s aktualizaci anebo když je v nové aktualizaci zabezpečení závada, zařízení se nemůže k VPN

znovu připojit, takže následně je nutná lokální změna konfigurace. Pokud na každé pobočce není přítomen zaměstnanec, který je schopen ručně zařízení znovu připojit, dojde k závažným problémům.

Architektura s okruhy se nejvíc hodí pro stabilní podniky, které nezažívají rychlý růst a kde je provozní tok mezi jednotlivými lokalitami předvídatelný.

2.4.2 Hvězdicovitá VPN

Hvězdicovitá VPN soustřeďuje všechna nastavení sítě na jediném ústředním směrovači VPN. Jednotlivá vzdálená zařízení mají pouze jednu bezpečnostní asociaci na ústřední zařízení a vzdálení uživatelé se přidávají pouze do tohoto ústředního zařízení. Jakmile ustaví vzdálené zařízení připojení k centrálnímu zařízení, není nutná žádná další konfigurace. Tato typologie je zobrazena na obrázku 2.4.2-2.



Obr. 2.4.2-2 Hvězdicovitá VPN

Cenou za toto řešení je bohužel to, že všechny pakety musí procházet centrálním zařízením VPN, což podle geografického rozmístění sítě může způsobit, že pakety budou trávit na trase o mnoho milisekund více času, než v architektuře s okruhy, kde je propojení přímé. I centrální směrovač VPN bude navíc pro každé připojení vyžadovat dvojnásobné náklady na přenosovou kapacitu, protože se vlévá do stejné trasy a musí být připraven komunikovat plnou rychlostí se všemi připojeními. Centrální směrovač by měl mít k dispozici

přenosovou kapacitu, která se rovná dvojnásobku součtu všech dalších účastníků VPN – což je číslo, které může velmi rychle narůst příliš a prodražit se.

Navíc ještě centrální směrovač VPN musí být schopen směrovat interně mezi jednotlivými bezpečnostními asociacemi. Překvapivě mnoho zařízení VPN tuto schopnost nemá, takže pokud hodláme použít hvězdicovou architekturu, pečlivě si před nákupem prostudujeme dokumentaci od dodavatele.

Hvězdicová architektura je nejvhodnější pro malé a střední podniky, které mají jednu hlavní kancelář a několik poboček, protože v takovém prostředí stejně většina provozu putuje do centrální kanceláře a z ní.

2.4.3 Hybridní VPN

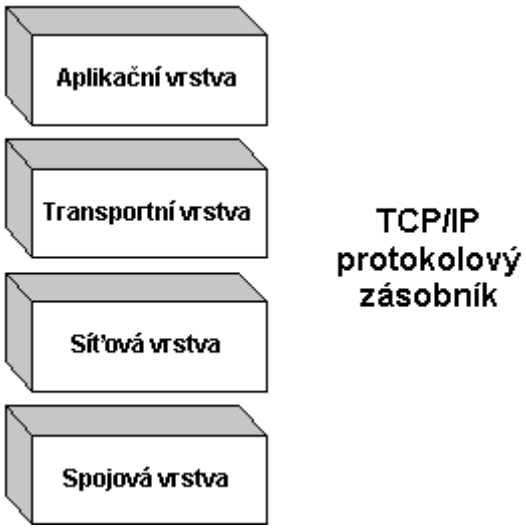
Hybridní VPN jsou pragmatickou kombinací hvězdicových VPN a VPN s okruhy. Většina implementací VPN se nakonec ve skutečnosti stane hybridními, ať už záměrně nebo náhodou během rozšiřování. Není v tom žádný problém a není důvod, proč dogmaticky trvat na jedné nebo druhé architektuře. Měly by se využívat v případech, kdy výhody z jejich silných stránek převáží nad nevýhodami pramenícími z jejich slabin.

Všeobecně řečeno by se v podniku mělo stabilní „jádro“ VPN implementovat jako síť s okruhy, a to kvůli sníženým nárokům na zatížení, které tato architektura má. Rozšíření podniku, rychlá rozšíření sítě, a vzdálení uživatelé by se měli zavádět na okrajích architektury s okruhy pomocí hvězdicových přípojek, aby jejich přidávání a vymazávání nemělo vliv na celou síť s okruhy. Nové odbočky lze pak přidávat k síti s okruhy v rámci aktualizace VPN každého půl roku, přičemž je možné na tuto dobu naplánovat dodatečnou podporu a připravit se na výpadek, ke kterému může v důsledku aktualizace dojít. Obecně řečeno by se nové pobočky měly vždycky přidávat jako paprsky k nejbližšímu rozbočovači a pak naplánovat všeobecnou aktualizaci - tj. integrovat všechny paprsky v pravidelných intervalech.

Vzdálení uživatelé by se měli vždy zavádět jako paprsky z rozbočovače a pokud tomuto řešení nebrání závažné překážky v podobě přenosové kapacity, pak by se měly vést z jediného směrovače VPN bez ohledu na to, odkud se geograficky připojují. Konektivitu vzdálených uživatelů lze centrálně řídit spravovat a v případě nutnosti i odpojit v jednom ústředním bodě VPN.

2.5 TYPOLOGIE SÍTÍ VPN

Existuje několik různých typů virtuálních privátních sítí (viz lit. [7]). V závislosti na požadavcích na funkcí sítě pak můžeme přistoupit k vybudování sítě daného typu několika způsoby. Rozhodnutí, který způsob zvolit, závisí na druhu problému, který má daná VPN řešit, požadavcích na míru bezpečnosti sítě, požadavcích na škálovatelnost řešení a náročnosti na implementaci, správu a údržbu.



Obr. 2.5-3 Protokolový zásobník TCP/IP

Nejnázornější rozdělení typů VPN se dá provést podle pohledu na funkčnost sítě v relaci s jednotlivými vrstvami protokolového zásobníku TCP/IP, viz obr. 2.5-3. Rozeznáváme tak:[6]

- **VPN na síťové vrstvě.** Síťová vrstva obsahuje informace, podle kterých probíhá směrování IP protokolu a práce se směrovacími informacemi je základem pro vytvoření VPN na síťové vrstvě. Typy VPN na síťové vrstvě:
    - filtrování směrovacích informací;
    - tunelování;
    - šifrování na síťové vrstvě.

- **VPN na spojové vrstvě.** Přenosový síťový systém je použit pro spojení na fyzické a spojové vrstvě, tato síť je funkční analogií konvenční privátní datové síti. Typy VPN na spojové vrstvě:

    - VPN v sítích LANE;
    - VPN v sítích MPOA;
    - VPN v sítích MPLS.

- **VPN se šifrováním na spojové vrstvě.**

- **VPN na transportní a aplikační vrstvě.** Tento typ sítí není příliš běžný, příkladem mohou být e-mailové systémy s kódovaným přenosem zpráv.

2.5.1 VPN na síťové vrstvě

Základem pro vytvoření VPN na síťové vrstvě je práce se směrovacími informacemi. Tyto informace, podle kterých probíhá směrování IP protokolu, obsahuje síťová vrstva(viz lit. [7]).

2.5.1.1 Filtrování směrovacích informací

Vytváření VPN s filtrováním směrovacích informací je založeno na jednoduchém principu omezení propagace směrovacích informací o dosažitelnosti jiných sítí. Tento model můžeme považovat za typ "peer ", protože jeden směrovač zastupující skupinu uzlů, patřících do VPN, navazuje spojení s předáváním směrovacích informací pouze se vstupním směrovačem sítě poskytovatele spojení a ne se všemi okolními sítěmi. Informace o dosažitelnosti vybrané sady sítí, tvořících VPN, tak není propagována okolním sítím, do dané VPN nenáležejícím. To samé platí i v obráceném směru.

2.5.1.2 VPN založené na tunelování

Další metoda budování VPN je založena na takzvaných tunelech. Jak název napovídá, při vytváření spojení mezi stroji ve VPN se (v nezabezpečené) části sítě vytvoří tunel, ve kterém pak komunikace probíhá a je od externí komunikace oddělena.

- **GRE tunely** jsou nejčastějším používaným způsobem klasického tunelování pro spojení zdrojového a cílového směrovače. Tyto tunely jsou budovány směrovači, které slouží jako vstupní a výstupní body do páteřní sítě pro jednotlivé části VPN. Speciálně zabalené pakety přenášené tunelem obsahují přídavnou GRE hlavičku (GRE Header) a cílovou adresu, odpovídající směrovači na konci tunelu. V koncovém bodě tunelu dojde k rozbalení paketu a následné směrování paketu do cíle již pokračuje podle informací ve své původní IP hlavičce. GRE tunely jsou obecně typu bod - bod, tzn., že pro tunel existuje jen jedna zdrojová a jedna cílová adresa.

- Další typ VPN s využitím tunelů, jsou sítě s komutovaným přístupem VPDN (Virtual Private Dial Networks). Tyto sítě se využívají u spojení VPN typ u klient – server. U sítí s komutovaným přístupem se využívají převážně dva standardy PPTP a L2TP, které budou popsány v kapitole 2.6.

2.5.2 VPN na spojové vrstvě

Technologie vytváření VPN na spojové vrstvě pracují na obdobném principu vytváření plně privátních sítí na vlastních nebo pronajatých oddělených přenosových linkách. Vytvořené VPN na spojové vrstvě jsou pak nezávislé na vyšší přenosové vrstvě. Infrastrukturu těchto sítí s virtuálními obvody na spojové vrstvě tvoří sítě ATM a Frame Relay. Za zvláštní typ VPN tvořených na spojové vrstvě můžeme považovat virtuální sítě (VLAN). Technologie virtuálních sítí vznikla původně pro prostředí ethernetových přepínačů, ale používá se i v sítích ATM a Frame Relay.

Konvenční privátní datové sítě používají kombinaci dedikovaných linek (obvodů), pronajatých od veřejného poskytovatele spojových služeb, a privátní komunikační infrastruktury. Tímto způsobem je vytvořena kompletní soběstačná síťová infrastruktura. VPN může být vytvořena v rámci jen této plně privátní infrastruktury, nebo ji může přesahovat. V případě, že přesahuje plně privátní strukturu, VPN se rozprostírá i po pronajatých, dedikovaných linkách (obvodech). Základní charakteristikou pronajatých dedikovaných linek (obvodů) od poskytovatele spojových služeb je nějaký způsob využívání časového nebo frekvenčního multiplexingu a synchronizace vysílání a příjmu dat (synchronní přenosy). [7]

Základní rozdíl v architektuře mezi virtuálními a dedikovanými obvody spočívá v neexistenci časové synchronizace přenosů, navíc zde ani nemusí existovat dedikovaná přenosová cesta. Vysílající uzel také nemá apriori žádnou znalost dostupné přenosové kapacity virtuálního obvodu, protože ta je závislá na celkových požadavcích ostatních simultánních přenosů. Proto může na rozdíl od dedikovaných obvodů docházet k přetížení sítě tvořené virtuálními obvody. [7]

Významnou výhodou veřejných přepínaných sítí (sítí poskytovatelů přenosových služeb) je jejich velká flexibilita. Většina uživatelů si pronajímá virtuální obvody z ekonomických důvodů a součástí smlouvy je samozřejmě i dohoda o kvalitě poskytovaných služeb, která umožňuje specifikovat konkrétní technické parametry sítě podle požadavků zákazníka. [7]

V sítích Frame Relay se např. používá pojem CIR (Committed Information Rate), sloužící jako referenční hodnota pro kontrolu velikosti přenosové rychlosti ve vstupním bodu sítě. Překročí-li rychlost dohodnutou hodnotu CIR, vstupní rámce jsou sice dále sítí akceptovány, jsou ale označeny jako DE (Discard Eligible). Takto označené rámce pak mohou být jako první zahozeny, dojde-li na jejich cestě sítí k přetížení (je překročena max. vstupní rychlost na přepínači a dojte k přetečení vyrovnávacích pamětí). [7]

Výše uvedené charakteristiky sítí s virtuálními obvody platí i pro sítě ATM (Asynchronous Transfer Mode). Stejně jako u sítí Frame Relay, i u sítí ATM není používána synchronizace datových přenosů mezi vysílačem, sítí a přijímačem. Obdobně se i používá vstupní funkce na kontrolu rychlosti vstupního proudu buněk, které mohou být označeny v případě překročení dohodnuté rychlosti indikátorem CLP (Cell Loss Prority) a při přetížení sítě jsou tyto buňky jako první zahozeny. [7]

Architektura sítí s virtuálními obvody na spojové vrstvě nabízí vysoce kvalitní alternativu k sítím pevných dedikovaných obvodů. Různé technologie pak umožňují využití těchto sítí různými způsoby, třeba až po přímou emulaci pevných linek při nutnosti konstantní přenosové rychlosti a garantovaného max. zpoždění. [7]

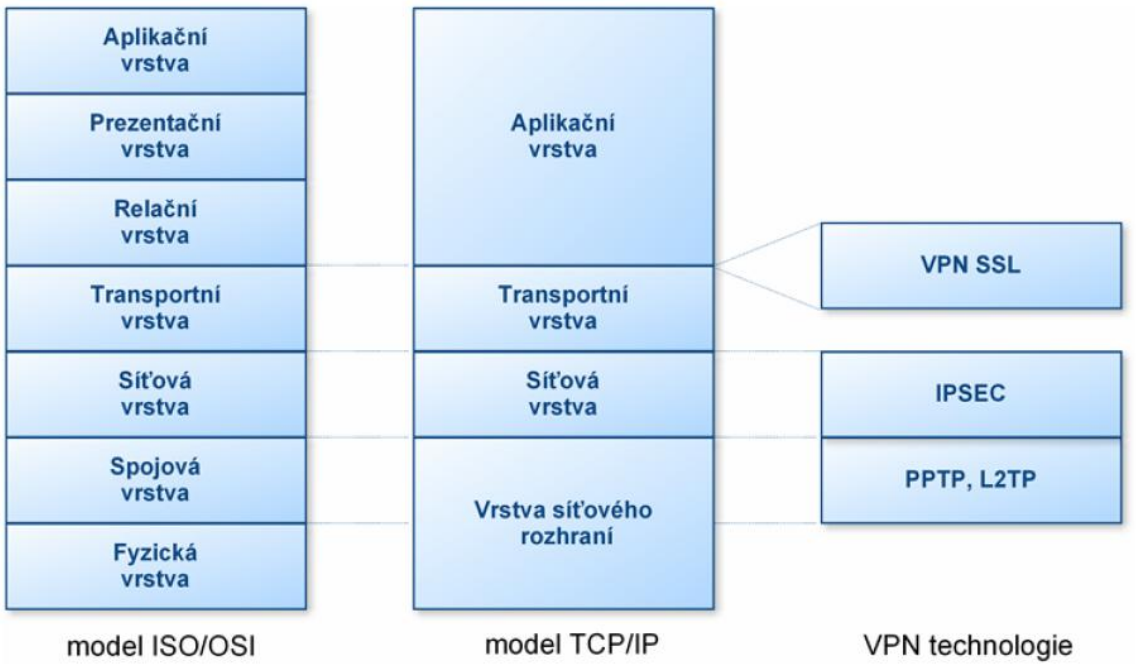
2.6 BĚŽNÉ IMPLEMENTACE VPN

I když teoreticky vzato lze VPN vytvořit pomocí jakéhokoliv silného šifrovacího algoritmu a nějaké formy zapouzdření IP, objevilo se na trhu několik špičkových implementací, které jsou oblíbené buď proto, že je lze spojit dohromady pomocí několika samostatných stávajících nástrojů, protože mnoho malých dodavatelů se na nich dohodlo jako

na společné normě anebo protože je implementuje velký dodavatel a začlenil je zdarma do různých svých univerzálních produktů, např. operačních systémů (viz lit. [3]).

Mezi běžné implementace VPN patří:

- **IPSec – režim tunel**
- **PPTP**
- **L2TP**
- **PPP/SSH nebo PPP/SSL**



Obr. 2.6-4 Technologie VPN v síťovém modelu

V dalších částech tyto jednotlivé běžné implementace popíšu podrobněji.

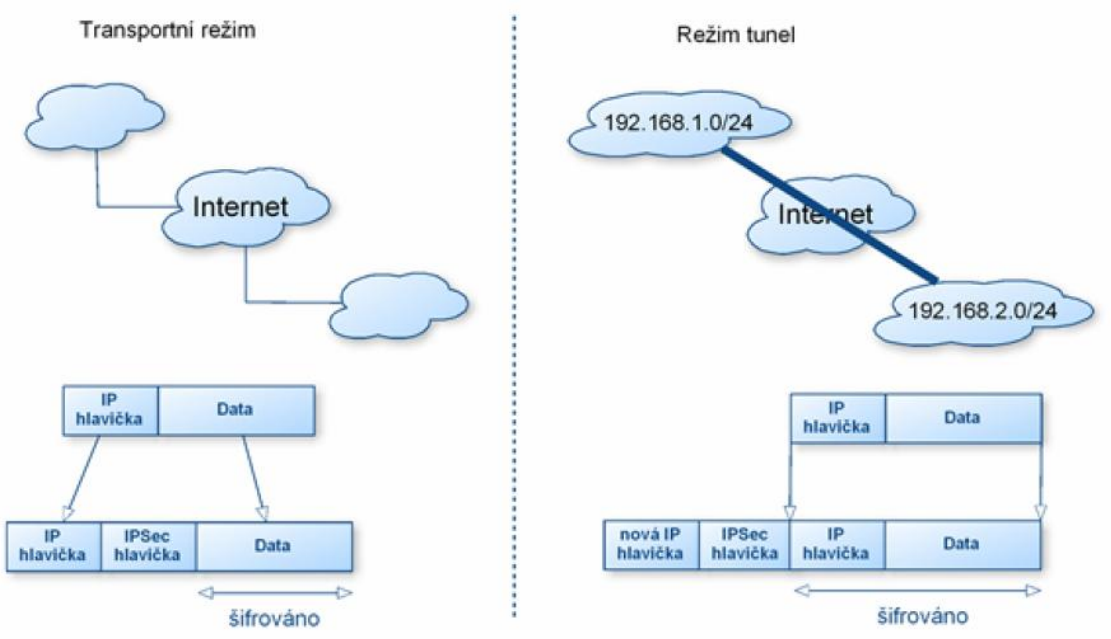
2.6.1 IPSec

IPSec je možné použít pro šifrování dat, přenášených skrze tunel vytvořený na jiném protokolu, například L2TP. Můžeme jej také použít k vybudování tunelu, pokud tento protokol pracuje v tunelovém režimu. V tunelovém režimu může být IPSec použit pro

zapouzdření IP paketů a může být nakonfigurován na ochranu dat mezi dvěma IP adresami nebo mezi dvěma IP podsítěmi.

IPSec může použít jeden nebo oba ze dvou protokolů: Authentication Header (AH) a Encapsulating Security Payload (ESP).

Protokol umožňuje 2 režimy: transportní režim a režim tunel (viz. obr. 2.6.2-5)



Obr 2.6.2-5 Režimy protokolu IPSec

2.6.2 PPTP

Point-to-Point Tunneling Protocol je protokol tunelového propojení, který pracuje na 2. vrstvě ISO/OSI referenčního modelu. PPTP Microsoftu je uznávaný standard, který je rozšířením linkového protokolu PPP, používaného k vytváření linek WAN přes vzdálené připojení. Zde je popis, jak pracuje:

1. PPTP zapouzdří PPP rámec, který může být IP, IPX nebo NetBEUI paketem uvnitř Generic Routing Encapsulation (GRE) hlavičky. Pro poskytnutí zdrojové a cílové IP adresy je vložena i IP hlavička. Zdrojová adresa je VPN klienta a cílová adresa je VPN serveru.
2. Data v originálním datagramu jsou normálně šifrována, takže je neautorizované osoby nemohou přečíst. Zabezpečenou komunikaci ve

virtuálních privátních sítích Microsoftu poskytuje MPEE protokol v kombinaci s protokolem PPTP.

PPTP-Linux je klientský software, který běhá na počítačích s operačním systémem Linux nebo UNIX a umožňuje připojení k PPTP serverům. Software PPTP server (nazývaný PoPToP) je dostupný pro Linux, Sun Solaris, FreeBSD a další implementace UNIXu. Tento software je volně šířitelný a klienty Windows podporuje stejně dobře, jako klienty PPTP Linux. Klienti Macintosh se mohou k Windows PPTP serveru připojit díky programům třetích stran, jako například Network Telesystem TunnelBuilder.

2.6.3 Protokol pro režim tunel na vrstvě 2 (L2TP)

Layer Two Tunneling protocol je protokolem tunelového připojení. Společnosti Cisco a Microsoft spojily výhody PPTP a L2F a vytvořily L2TP. L2TP může odesílaná data zapouzdřit pro odeslané přes IP síť stejně jako PPTP. L2TP také může data zapouzdřit pro odeslání skrze ATM, Frame Relay a X.25. Z toho důvodu je možné jej použít k vybudování tunelu skrze Internet. Zde jsou některé výhody L2TP před PPTP:

- L2TP podporuje vytvoření více tunelů mezi koncovými body. Tím je možné vytvořit několik oddělených tunelů.
- L2TP podporuje komprimaci hlaviček.
- L2TP je oproti PPTP schopný autentizovat tunel.
- L2TP pracuje na ne-IP sítích použitím virtuálních obvodů ATM nebo FrameRelay.

2.6.4 PPP/SSL nebo PPP/SSH

Dvěma běžnými metodami kterými administrátoři instalací unixových a *open - source* operačních systémů vytvářejí VPN „za pochodu“ jsou PPP (Point to Point Protocol) přes SSL (Secure Socket Layer) nebo SSH (Secure Shell). Obě metody, které by se ve světě Windows mohly považovat za „hackerské pokusy“, používají chytré propojení stávajících transportních vrstev (SSL nebo SSH) a stávajících tunelů (PPP)

2.7 BEZPEČNÝ VZDÁLENÝ PŘÍSTUP

Virtuální privátní sítě jsou výborným nástrojem na propojování sítí LAN, ale co s lidmi s izolovanými počítači, např. lidé pracující z domova, mobilní řešitelé problémů, obchodní zástupci, vedoucí pracovníci na cestách nebo všichni ti šťastní (nebo nešťastníci), kteří nemusí pracovat v kancelářích (viz lit. [3]) .

Tradiční (drahou) metodou, jak poskytnout těmto uživatelům přístup na LAN, je nainstalovat modemové banky a zakoupit telefonní linky, aby se mohli k síti LAN připojovat přes modemy vytáčeným připojením. Takto poskytované služby s vytáčeným připojením vyžadují modem a telefonní linku pro každé souběžné připojení. Pokud se tedy mají současně připojit dva lidé, jsou potřeba pro server s vytáčeným připojením dva modemy a dvě telefonní linky. Pokud má být připojení poskytnuto najednou dvěma stům lidí, bude zapotřebí dvě stě modemů a dvě stě telefonních linek (a navíc ještě vybavení na sériová připojení). Dále bude muset firma nebo uživatel vytáčeného připojení platit veškeré meziměstské poplatky za telefon, pokud nebudou uživatelé a server pro vytáčené připojení v oblasti stejného místního, městského tarifu.

Téměř všude v průmyslové části světa je v současnosti k dispozici v rámci městských tarifů poskytovatel internetového připojení. Ceny internetových služeb od těchto poskytovatelů jsou relativně nízké, protože ISP mohou rozdělit náklady na podporovaná vytáčená připojení na širokou základnu zákazníků. Pro připojení ve vlastní síti je smysluplné těchto služeb vytáčeného připojení využít a ne je zdvojovat. Ale problém spočívá v tomto: Jak lze zabezpečit komunikace přes síť mezi vzdálenými počítači a počítači v síti LAN?

Rozšířit virtuální privátní na jednotlivé vzdálené počítače, které se připojují přes Internet, lze dvojím způsobem. Buď se uživatelé nechají, aby se připojovali přes ISP (kteří mají k dispozici v rámci svých služeb port pro VPN), takže ISP se bude v podstatě podílet na správě a zabezpečení sítě LAN. Anebo se port VPN přesune na vzdálený počítač.

2.7.1 VPN u ISP

Poskytovatelé internetového připojení připojují ke svým sítím s vytáčeným připojením modemy a telefonní linky zvláštními zařízeními, kterým se říká přepínače pro vzdálený přístup, servery pro vzdálený přístup, terminálové servery, nebo koncentrátory sériových propojení. Koncentrátory sériových propojení umožňují počítači se serverem (často se jedná o vyhrazený směrovač VPN nebo hostitelský počítač na platformě Unix, ale někdy i server na

platformě Windows), aby přijímaly velké množství vytáčených připojení. Přepínače a servery pro vzdálený přístup a terminálové servery jsou specializované počítače, které provádějí pouze připojování volajících účastníků k síti. Každopádně server s vytáčeným připojením (nebo jakýkoliv specializovaný počítač nebo zařízení) provádí autentizaci uživatele a připojení počítače uživatele k síti LAN uvedeného ISP. [3]

Společnost Cisco, Microsoft a mnoho dalších dodavatelů je přesvědčeno o bezpečnosti protokolu, kterému se říká L2TP. Když si uživatel založí účet u ISP, může uvést (ve spolupráci s administrátorem sítě LAN, ke které se chce připojit) sítě VPN, do kterých by měl mít jeho počítač povolen přístup. Když se uživatel připojí na přepínač pro vzdálený přístup (obvykle přes protokol PPP), přepínač u ISP nejprve u sebe vyhledá uživatelské jméno a heslo uvedeného uživatele a pak přes Internet ustaví zašifrované připojení na server RRAS, který uvede administrátor sítě uživatele. Vzdálený uživatel se pak může (samozřejmě poté, co pro uvedenou LAN sdělí platné jméno účtu a heslo) připojit na LAN jako všechny další klientské počítače připojené k síti.

Když svěříte ISP, aby ustavil propojení zašifrovaným tunelem a autentizoval a zapouzdřoval síťový provoz vzdálených uživatelů, budete mít stejné zabezpečení jako když svěříte ISP sítě LAN, aby za vás spravoval firewall. Mnoho společností svěřuje provádění funkcí firewallu poskytovatelům internetového připojení, což je snad levné řešení, pokud ovšem důvěřují zabezpečení a spolehlivosti uvedeného poskytovatele. [3]

2.7.2 VPN v klientském počítači s vytáčeným připojením

Ve většině případů nemá vzdálený uživatel možnost svěřit ustavení relace VPN poskytovateli internetových služeb. Valná většina dodavatelů firewallů a zašifrovaných tunelů nabízí software pro tunely ve verzích pro malé klientské systémy, které lze spustit přímo na klientském počítači vzdáleného uživatele. Klient se tak může přímo připojovat k firewallu přes Internet a vše může vypadat, jako by se jednalo o pracovní stanici na lokální síti. [3]

Klientský počítač se potřebuje k ustavení relace VPN nejprve připojit k internetu. Lze to provést buď přes libovolného ISP nebo dokonce i z počítače na jiné síti LAN (která není součástí VPN) připojené k Internetu. Jakmile se dostane klientský počítač na Internet, software pro VPN na klientském počítači může ustavit zašifrované připojení k firewallu nebo na server, který používá TCP/IP. [3]

Je ale potřeba mít se na pozoru před skrytými problémy při překládání síťových adres, ke kterým dochází u IPSec. U IPSec nelze použít překládání síťových adres (dobrá,

u jediného připojení IPSec, které používá pouze ESP v režimu tunel, je to možné, ale u více než jednoho nikoliv). To některým mobilním uživatelům působí vážné problémy, protože hotely, které poskytují internetové služby, často zavádějí překládání síťových adres, aby si rozšířily kapacitu adres IP. Poskytovatelé satelitního připojení a jiných alternativních možností přístupu zavádějí oddělené směry toků dat (upload /download), které se neslučují s řádným fungováním IPSec na klientských počítačích. [3]

Pokud vzniknou takové problémy, je asi dobré zvážit možnost použití protokolu PPTP. Ačkoliv není úplně nepropustný, Microsoft v něm většinu nejzávažnějších nechvalně známých problémů odstranil a na rozdíl od ostatních metod vzdáleného přístupu se PPTP dobře přes NAT překládá a může fungovat téměř na jakémkoliv připojení IP, bez ohledu na různé triky, které se pro připojení k Internetu ve skutečnosti použijí. Tohle je asi jediný důvod, proč by šlo využití PPTP doporučit. [3]

3 ANALÝZA SOUČASNÉHO STAVU

3.1 OBJEKT ŘEŠENÍ

3.1.1 O firmě Lázně Darkov, a.s.

Lázně Darkov se nacházejí na severovýchodě České republiky. Tvoří je dvě léčebná zařízení (viz lit. [17]):

- Léčebna Darkov v Karviné–Darkově
- Rehabilitační sanatorium v Karviné–Hranicích.

Díky vysoké úrovni léčby, která je založená na mimořádném přírodním bohatství jodobromové vody s vysokým obsahem jódu, profesionalitě zaměstnanců a kvalitě doplňkových služeb se Lázně Darkov řadí mezi vyhledávaná lázeňská zařízení.

Vznik Lázní Darkov je připisován roku 1867, kdy byla zahájena 1. lázeňská sezóna. Založení lázní předcházelo vědecké prozkoumání přírodního léčivého zdroje, jodobromové vody solanky, kterou již dříve znali místní lidé v podobě léčivé studánky a využívali ji v přírodním léčitelství.

Postupem času bylo zjištěno, že vzácná voda s vynikajícími účinky, zejména pro léčbu pohybového ústrojí a cévního systému, má mořský třetihorní původ a plným právem byla nazvána darem z hlubin země.

Věhlas lázní se velmi rychle šířil. Od roku 1895 - 1902 byla budována další ubytovací zařízení, jelikož první dvě budovy již nedostačovaly. Založen byl i lázeňský park se vzácnými dřevinami.

Další výstavba následovala až v r. 1931. S výjimkou dvou světových válek, kdy se prostory proměnily ve vojenský lazaret, sloužily Lázně Darkov po celou dobu svému účelu. Posledním jejich majitelem před rokem 1945 byl hrabě Larisch - Mönnich, pak se staly na dlouhou dobu majetkem státu.

Jelikož solanka je uložena ve výdutích uhelné pánve, musely lázně čelit vlivům důlní činnosti a po určitý čas hrozil lázním zánik. Proto bylo přistoupeno k výstavbě nových objektů na opačném předměstí města Karviné. Tento nový areál vzájemně propojených budov byl postupně zprovozněn v letech 1976, 1980 a 1989 pod názvem Rehabilitační sanatorium.

Budovy se vyznačovaly architektonickou strohostí dané doby, ale svým prostorovým vybavením rozšířily možnost léčby pro imobilní klienty u zcela nových diagnóz, zejména stavů po mozkových příhodách, úrazech i operacích pohybového ústrojí.

Obě lázeňské části, Léčebna Darkov i Rehabilitační sanatorium, působily jako jeden ekonomický celek státního podniku. Původní lázeňské budovy díky pozastavení důlní činnosti mohly být po roce 1989 postupně zrekonstruovány i zmodernizovány, a nyní všechny v maximální míře odpovídají požadavkům dnešního standardu. Některé z budov byly pro svou architekturu vyhlášeny kulturní památkou a lázeňský park, rovněž zrekonstruovaný, byl označen jako významný krajinný prvek.

Od 1. 9. 2003 se Lázně Darkov staly akciovou společností, která ve své činnosti navázala na 135letou tradici významných lázní. Velkými investicemi do modernizace společnost usiluje o další zkvalitnění a zatraktivnění prostředí.

3.1.1.1 Léčebna darkov

Léčebna Darkov byla od svého vzniku v roce 1867 až do roku 1976 jediným léčebným zařízením Lázní Darkov. Léčí se zde klienti s poruchami pohybového a oběhového ústrojí. Tvoří je osm budov, vyhlášených za kulturní památky. Nacházejí se v krásném prostředí lázeňského parku, založeném v roce 1900, jenž je registrován jako významný krajinný prvek a skýtá velmi příjemné, klidné prostředí, vybízí k procházkám i odpočinku.¨

3.1.1.2 Rehabilitační sanatorium

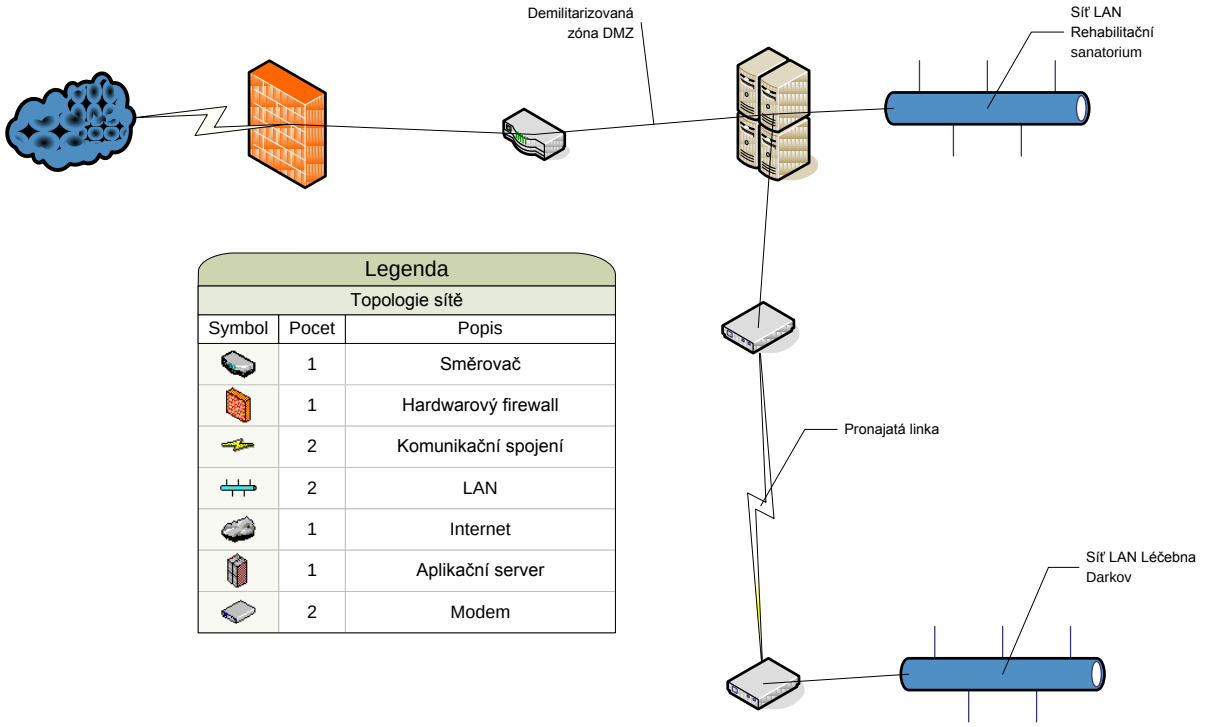
Komplex Rehabilitačního sanatoria navázal na bohatou tradici Léčebny Darkov a od r. 1976 poskytuje špičkovou lázeňskou péči, zaměřenou na léčbu pohybového ústrojí, zejména stavů po operacích a úrazech, neurologických onemocnění, stavů po popáleninách. Jedná se o bezbariérový komplex vzájemně propojených budov, usnadňujících pobyty také imobilním klientům, je obklopen lázeňským parkem.

3.2 FIREMNÍ POČÍTAČOVÁ SÍŤ, SOUČASNÝ STAV

3.2.1 Hardwarové vybavení sítě

Firemní počítačová síť řešeného podniku, je založena na síťových technologiích firmy Cisco. Topologie firemní sítě se skládá z a je zobrazena na obrázku 3.2-6:

- hardwarového firewallu,
- hlavního směrovače,
- serveru,
- dvou oddělených sítí LAN, které představují sítě pracoviště Rehabilitačního sanatoria a Léčebny Darkov
- a jedné sítě typu WAN která propojuje tyto dva pracoviště.



Obr. 3.2-6 Topologie sítě

3.2.1.1 Hardwarový firewall

Firewall je síťové zařízení, které slouží k řízení a zabezpečování síťového provozu mezi sítěmi s různou úrovní důvěryhodnosti a zabezpečení. Zjednodušeně se dá říct, že slouží

jako kontrolní bod, který definuje pravidla pro komunikaci mezi sítěmi, které od sebe odděluje. Pomocí firewallu je dosaženo nejbezpečnějšího připojení k Internetu. Firewall kontroluje nebo zamítá jednotlivé pokusy o připojení mezi interní a externí síti jako je třeba Internet.

V současnosti firma používá hardwarový firewall společnosti Cisco řady ASA 5500 Series Adaptive Security, který poskytuje inteligentní ochranu proti útokům a vysokou bezpečnost komunikačních služeb.

Funkce firewallu:

- Adaptivní architektura a cílené bezpečnostní služby.
- Pokročilé služby pro prevenci narušení, které chrání před řadou hrozeb
- Vysoce zabezpečený vzdálený přístup

3.2.1.2 Hlavní směrovač (router)

Směrovač je základním kamenem síťového provozu. Bez směrovače by nemohl existovat ani Internet, jak jej všichni známe. Důvodem této důležitosti směrovačů jsou jejich následující jedinečné a silné funkce:

V současné době je ve firemní síti použit jako hlavní směrovač zařízení společnosti Cisco 2811 Series Integrated Services Router, který se vyznačuje těmito vlastnostmi:

- Bezdrátová síť: Usnadňuje zaměstnancům dosažení vyšší produktivity a lepší spolupráce zajištěním možnosti pracovat bezdrátově odkudkoli v kanceláři.
- Hlasové služby: Pokročilé komunikační nástroje včetně zpracování telefonních hovorů, hlasové pošty, funkce Automated Attendant a konferenčních funkcí vám pomohou rychleji reagovat na požadavky zákazníků a ušetřit peníze za meziměstské a mezinárodní hovory.
- Video: Má možnost zřídit rentabilnější dohlížecí a bezpečnostní systémy nebo podporovat média spouštěná na vyžádání a živé datové proudy.
- Zabezpečení: Snižuje podnikatelská rizika související s viry a jinými bezpečnostními hrozbami.

- Virtuální privátní sítě: Zaměstnancům na odlehlých pracovištích nebo pracujícím z domu můžete poskytnout bezpečný přístup k firemním prostředkům přes zabezpečené připojení.
- Modulární architektura: Díky široké škále možností pro sítě LAN a WAN možnost upgradovat síťová rozhraní a začlenit do nich budoucí technologie. Řada 2800 Series nabízí rovněž několik typů slotů, díky kterým se usnadní budoucí rozšíření možností připojení a služeb – a to na principu „integrace synchronní s růstem“.
- Flexibilita: Připojení přes linku DSL, kabelový modem, připojení T1 nebo bezdrátovou linku 3G maximalizuje možnosti pro primární i záložní připojení.

Router Cisco 2811 Series Integrated Services Router nabízejí řadu funkcí, mezi které patří: integrované zabezpečení, jako je firewall, šifrování a ochrana před hackery, pro větší ochranu má integrovaný konektor pro redundantní zdroj napájení, je u něj zvýšená spolehlivost a flexibilita umožňující nastavit prioritu hlasových přenosů nebo výměny dat, aby doručování informací bylo v souladu s firemními potřebami, podporuje pokrytí bezdrátovou sítí LAN pro celé kanceláře s účinnými funkcemi zabezpečení a přístupu pro hosty a s možností použití všech aktuálních bezdrátových standardů: IEEE 802.11a/b/g/n, podporuje celou řadu variant síťového a širokopásmového připojení a aby se snížily náklady na kabeláž je ho možno napájet ze síťových zařízení přes připojení Ethernet (Power Over Ethernet).[12]

3.2.1.3 Demilitarizovaná zóna

Demilitarizovaná zóna je komplexnější řešení, plnící roli firewallu. Je založena na použití určitého "mezistupně" mezi oběma světy, které jsou řízeným způsobem propojeny - tedy mezi chráněnou podnikovou sítí, a nechráněným Internetem. Tento mezistupeň má charakter malého samostatného síťového segmentu, který je "viditelný" z každé z obou stran, ale není "průhledný skrz": díky způsobu, jakým je propojen s podnikovou sítí i se samotným Internetem je možný pouze takový provoz, který začíná či končí v tomto "mezistupni", ale žádný provoz nemůže projít "skrz" něj. V odborné terminologii se tomuto mezistupni říká trefně "demilitarizovaná zóna", neboť skutečně slouží jako určité nárazníkové pásmo mezi oběma okolními světy.

3.2.1.4 Server

Server poskytuje služby klientům, což označujeme jako model klient-server Lokální službou může být například obsluha připojené tiskárny, správa automatických aktualizací a podobně.

Služby, které firemní server poskytuje v lokální síti (LAN) je sdílení disků, tiskáren nebo schopnost ověřit uživatele podle jména a hesla (autentizace).

Firemní server pracuje na platformě Windows Server 2003, Enterprise Edition. Poskytuje funkce potřebné k zajištění provozu podnikové infrastruktury.

Na serveru je umístěn softwarový firewall, který je součástí operačního systému Windows Server 2003.

Použitý hardware:

- CPU: 2x čtyřjádrová Intel Xeon 1.8 Ghz
- RAM: 3x 2GB DDR3 800 Mhz
- HDD: 2x 1 000 MB/7200 rpm
- LUNA PCI - 3000 + PED

3.2.1.5 Sítě LAN

Firemní síť se skládá ze dvou od sebe oddělených sítí LAN jedna funguje v Rehabilitačním sanatoriu a druhá síť funguje v Léčebně Darkov.

Síť se skládá z aktivních a pasivních prvků. Aktivní prvky se aktivně podílejí na komunikaci. Patří mezi ně switche, routery, síťové karty apod. Pasivní prvky jsou součásti, které se na komunikaci podílejí pouze pasivně (tj. nevyžadují napájení) – propojovací kabely (strukturovaná kabeláž, optické vlákno, koaxiální kabel). Ve firemní síti je jako kabeláž použita kroucena dvoulinka, která je v dnešní době zdaleka nejrozšířenějším druhem LAN kabeláže

Lokální síť používá IP adresaci 10.0.0.0 protože toto řešení umožňuje větší míru pružnosti pro přidělování IP adres. Jelikož jsou obě firemní lokální sítě odděleny, každá používá svoji adresaci.

Standardní maskou podsítě je maska 255.255.0.0., jde o adresu typu B, na které může pracovat více než 65 000 počítačů.

3.2.1.6 Síť WAN

Pro spojení lokálních sítí obou pracovišť tj. Rehabilitačního sanatoria a Léčebny Darkov je použito spojení pomocí pronajaté linky. Na rozdíl od vytáčené linky jsou permanentně spojené tyto lokální sítě. Jeden modem je nakonfigurován jako volající a druhý jako odpovídající. Jakmile je spojení navázáno data mohou být kontinuálně vysílána k příjemci. Jestliže je nějaký problém na lince, či s napájením, modem po obnově automaticky naváže spojení. Roční náklady za pronájem linky = 180 000,- Kč bez DPH s rychlostí 20Mbit/s. Pomocí této pronajaté linky, je také zajišťován přístup k Internetu, protože k Internetu je připojeno pouze Rehabilitační sanatorium.

3.2.2 Připojení k Internetu

Počítačová síť řešeného podniku, je k Internetu připojena bezdrátovou sítí s garantovanou přenosovou rychlostí. Toto připojení je zřízeno pomocí bod-bod vyhrazeného spoje a je zřízeno místním dodavatelem Internetu. Přenosová rychlost dosahuje 100 Mbit/s za 100 000,-Kč bez DPH ročně. Tímto připojením je vybaveno pouze Rehabilitační sanatorium. Druhé pracoviště, tzn. Léčebna Darkov, používá pro připojení k Internetu pronajatou linku, kterou je připojena k Rehabilitačnímu sanatoriu.

3.2.3 Zhodnocení analýzy

Při analýze sítě a jejich hlavních prvků topologie jsem vycházel především z osobních konzultací s IT manažerem řešeného podniku Lázně Darkov a.s.

Z analýzy jsem zjistil, že k propojení pracovišť Rehabilitačního sanatoria a Léčebny Darkov, je použita zastaralá a podle mého názoru dražší technologie propojení poboček, pomocí pronajaté linky.

Dále jsem zjistil, že se ve firmě nepoužívá vzdálený přístup k počítačové síti pomocí virtuálních privátních sítí.

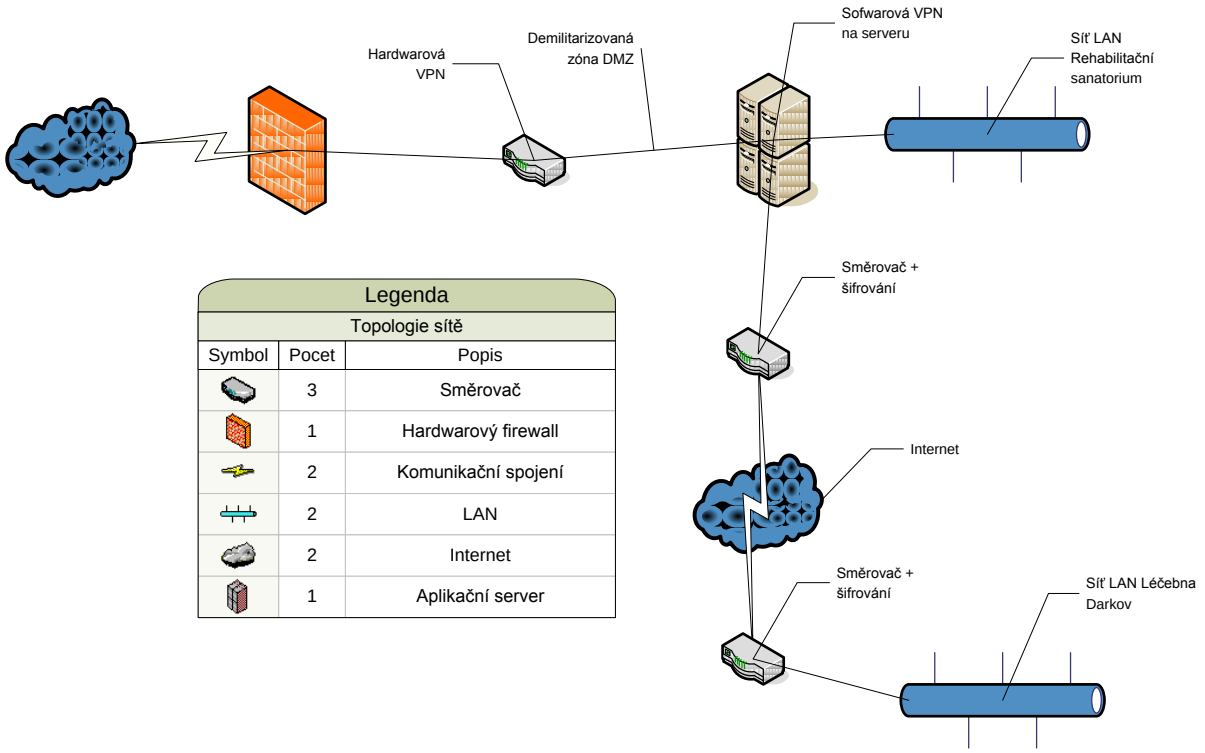
Proto se v další kapitole pokusím navrhnout ekonomicky výhodnější řešení propojení pracovišť a vzdáleného přístupu k počítačové sítí pomoci virtuálních privátních sítí.

4 NÁVRH RACIONALIZACE POČÍTAČOVÉ SÍTĚ

Virtuální privátní síť může být provedena hardwarově nebo softwarově. V této části diplomové práce se pokusím navrhnout využití virtuálních privátních sítí ve firemní síti a popsat produkty několika firem, které se zabývají řešením VPN.

Po předchozí analýze, kdy jsem zjistil, že lázně nevyužívají možnosti VPN, ačkoliv se u vzdáleného přístupu a propojení pracovišť Rehabilitačního sanatoria a Léčebny darkov přímo nabízí. Na obrázku 4-7 je zobrazeno nahrazení pronajaté linky VPN spojením a na serveru je nahráno softwarové řešení pro vzdálený přístup.

V dalších částech této kapitoly budou tato řešení popsána.



Legenda

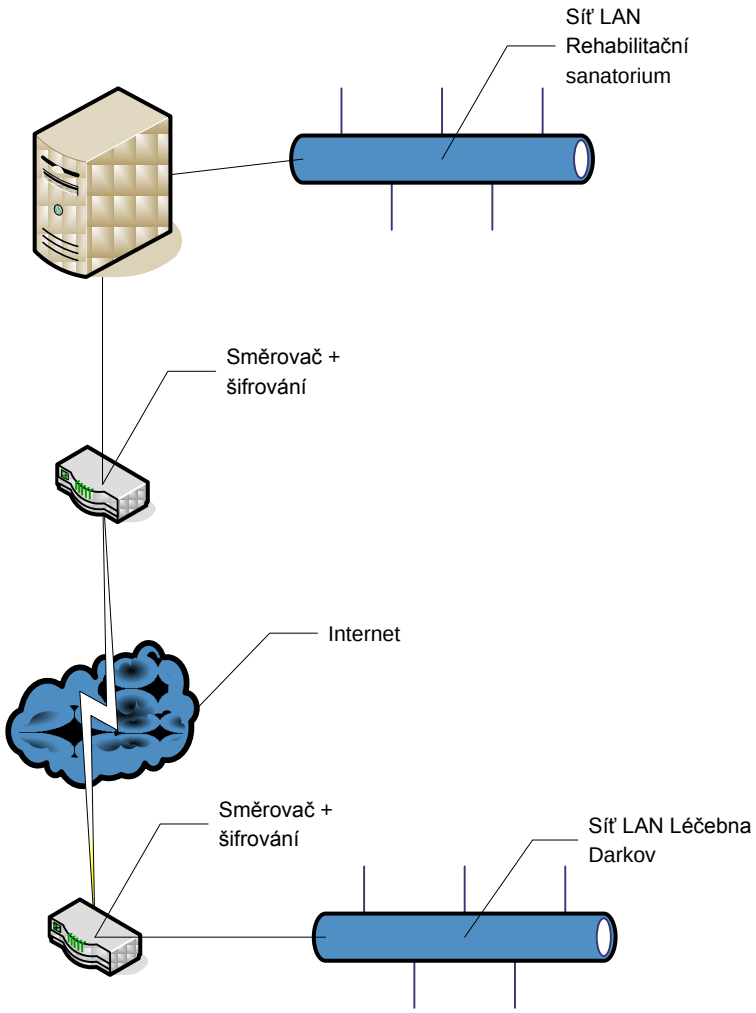
Topologie sítě

Symbol	Pocet	Popis
	3	Směrovač
	1	Hardwarový firewall
	2	Komunikační spojení
	2	LAN
	2	Internet
	1	Aplikační server

Obr. 4-7 Topologie racionalizované sítě

4.1 HARDWAROVÉ ŘEŠENÍ PROPOJENÍ PRACOVIŠŤ REHABILITAČNÍHO SANATORIA A LÉČEBNY DARKOV

Pro VPN propojení dvou vzdálených pracovišť se používá konfigurace router - router (směrovač-směrovač). Této konfiguraci se taky někdy říká gateway - gateway a je to hardwarové řešení. Jak je vidět na obrázku 4.1-8, VPN připojení router - router, propojí dva vzdálená pracoviště.



Obr 4.1-8 Propojení vzdálených pracovišť konfigurací router - router

Lokální síť v obou vzdálených pracovištích bude mít směrované připojení k Internetu. Toto připojení může být navázáno, buď podle potřeby a nebo permanentně. U připojení podle potřeby by směrovač používal iniciující spojení, telefonické připojení k Internetu. Volaný směrovač, ten ve vzdálené pobočce by pak musel mít vyhrazené připojení k Internetu (pevné připojení) a musel by být nastaven na příjem příchozích volání na požádání. Na volajícím

směrovači, jsou nastaveny dvě připojení na požádání, jedno pro připojení k poskytovateli Internetu a druhé pro připojení k virtuální privátní síti. Pokud oba směrovače mají vyhrazené připojení k Internetu, může být VPN podle potřeby trvale navázané. VPN v konfiguraci směrovač-směrovač může být také nastaveno tak, že jeden router je klient a zahajuje připojení a druhý pracuje jako VPN server . Toto je jednosměrné připojení a u permanentního připojení se jeví jako dobrá volba. Další možností propojení typu směrovač-směrovač je obousměrné připojení, kde může komunikaci zahájit kterýkoliv směrovač. V takovém případě musí mít oba směrovače trvalé připojení k Internetu a musí být nastaveny jako LAN a WAN směrovače.

4.1.1 Hardwarové VPN

Hardware pro virtuální privátní sítě vyrábí například společnosti Shiva, 3Com a VPNet Technologies. Podpora VPN je vestavěná v routerech Cisco, stejně jako v routerech ostatních výrobců. NTS TunnelBuilder poskytuje zabezpečenou komunikaci po VPN pro Windows, NetWare a Macintosh. Výrobci firewallů, jako například Raptor Systems, nabízejí VPN, které jsou založené na firewallech a jsou zkombinované s bezpečnostními nástroji. Trh se síťovým harwarem je strašně dynamický a každou chvíli přichází na trh nový dodavatel. Nicméně nedoporučuji používat nové produkty jen proto že jsou nové a levné ale hlavně jsou nevyzkoušené a to může nest se sebou bezpečnostní hrozbu. Hardwarové VPN můžeme obecně rozdělit do následujících skupin:

- Založené na routeru - Řešení VPN založené na routeru jsou vlastně routery se schopností šifrování. Poskytují nejlepší výkonnost sítě a celkem snadno se nastavují a používají.
- Založené na firewallu - Řešení založené na firewallu poskytuje zvláštní bezpečnostní opatření, jako silnou autentizaci a ukládání detailních logů. VPN založená na firewallu může také provádět překlad adres NAT. Výkonnost může být sporná, ačkoliv u některých implementací tento problém řeší procesory pro hardwarově založené šifrování.

4.1.2 Návrh variant

Hardwarové řešení společnosti CISCO

Funkce virtuálních sítí VPN jsou vestavěnou součástí modelových řad směrovačů Cisco. Přístupový směrovač Cisco 2800 Series Integrated Services Routers slouží například pro připojení malých vzdálených pracovišť do sítě VPN; je proto postaven tak, aby v jediném balíku nabízel vysokorychlostní šifrování a služby směrování tunelů. Pokud má síť VPN pracovat přes PIX Firewall, je nutné nakonfigurovat zvláštní povolený průchod.[4]

Virtuální privátní sítě bývaly tradičně výhradně softwarových řešením. Dnes se ale na trh dodávají speciální zařízení, navrhovaná právě s ohledem na potřeby funkcí VPN, takže i služby sítí VPN jsou dokonalejší než jen při čistě sofwarovém řešení. Doplněním funkcí VPN do směrovačů řad Cisco 2600, 2800 a 3600 se například výkonnost sítě VPN zvýší proti samotnému softwarovému řešení až desetinásobně.[5]

Hardwarové řešení společnosti Juniper

Juniper Network Secure je jedním z dominantních výrobcu SSL VPN produktů. Juniper Networks SSL jsou založeny na Instatnt Virtual Extranet (IVE) platformě, která používá SSL bezpečnostní protokol, který je součástí webových prohlížečů. Tyto produkty podporují jak OpenSSL tak webovské proxy metody SSL VPN, které jsou k dispozici pomocí volitelného upgrade přístroje.

Kromě SSL-VPN zařízení, Juniper integruje VPN do svého NetScreen firewall produktu, který umožňuje řízení přístupu a ověřování síťové segmentace. Tím, že Juniper kombinuje firewall a VPN technologie, nabízí komplexní zabezpečení v jednom balíčku. Kromě toho jsou Juniper VPN technologie založené na IPSec protokolu, který je ideální pro propojení sítí. NetScreen je bohužel kompatibilní pouze s platformou Windows.

4.1.2.1 Výběr nejlepší varianty a cenová kalkulace

Po konzultaci s IT manažerem společnosti Lázně Darkov, jsme dospěli k názoru, že nejlepším řešením pro propojení pracovišť Rehabilitačního sanatoria a Léčebny Darkov, bude použití směrovačů Cisco, jelikož na této síťové technologií je postavena celá podniková síť, proto nebudeme brát v úvahu další řešení.

Cenová kalkulace

Pro propojení obou pracovišť bude potřeba zakoupit 2ks směrovačů Cisco 2800 Series Integrated Services Routers s cenou v zaokrouhlení 11 000,-Kč bez DPH, lišící se podle zprostředkovávající firmy a zřízení bezdrátového připojení k Internetu s garantovanou rychlostí Léčebny Darkov s jednorázovou cenou aktivace 3000Kč bez DPH a ročním poplatkem 72 000,- Kč bez DPH za rychlost 40Mbit/s.

4.1.3 WAN vs. VPN

Jestliže se chystáme ve společnosti využít možnosti VPN, je důležité znát výhody a nevýhody (viz lit. [3]) porovnání se standardními sítěmi LAN a WAN a to zejména:

- VPN jsou levnější než WAN.
- Snadnější implementace VPN.
- VPN jsou pomalejší než WAN.
- VPN jsou méně spolehlivé oproti WAN.
- VPN jsou méně bezpečné než izolované LAN nebo WAN.

V dalších částech se pokusím uvedené vlastnosti blíže popsat.

4.1.2.1 VPN jsou levnější než WAN

V mnoha případech je prioritou číslo jedna skutečnost, že VPN je často mnohem levnější než síť WAN podobné velikosti, zvláště když se v síti LAN požaduje zavedení internetové konektivity. Jedna pronajatá vyhrazená linka mezi dvěma velkými městy je velmi drahá, a cena se odvíjí v závislosti na potřebné přenosové kapacitě a podle toho, na jakou vzdálenost musí být okruh vytvořen. Pomocí pronajaté linky tohoto druhu se obvykle ustavuje vyhrazené připojení společnosti k ISP, ale okruh je mnohem kratší – obvykle pouze několik kilometrů – a obvykle je už na místě nainstalováno připojení IP a je na něj vyhrazen rozpočet. U VPN se požaduje pouze jedná vyhrazená linka na ISP a lze ji využít jak pro internetový provoz tak i pro provoz VPN. Náklady lze snížit tak, že si zvolíme ISP, který se nachází co nejblíže sídlu společnosti.

Připojení podniku k Internetu přes ISP lze ustavit i pomocí běžných analogových modemů, ISDN, xDSL nebo kabelových modemů, podle služeb, které jsou v dané lokalitě dostupné. Tyto metody připojení k internetu mohou být daleko levnější než vyhrazené telefonní linky, ale je nutné si vyhodnotit, zda je pro použití ve VPN postačující přenosová kapacita, kterou tato připojení poskytují. Satelitní připojení se obvykle poskytují jako hybridní systémy, které často nejsou kompatibilní s náročnějšími šifrovacími protokoly jako IPSec, takže se s daným typem připojení ještě před tím, než si ho vyberete, podrobně seznamte.

Oproti tradičním sítím WAN síť VPN opravdu září v tom, jak se chová k sítím LAN, které propojují vzdálené, oddělené geografické oblasti (v různých městech, různých státech nebo dokonce i v jiných zemích). Náklady na vyhrazené meziměstské linky jsou mnohem vyšší než náklady na okruhy s místními smyčkami (tj. propojení mezi lokalitami, které se připojují ke stejné lokální telefonní ústředně). Protože místo drahých meziměstských linek lze VPN vytvořit i přes Internet, lze také vyloučit výdaje na meziměstské i městské okruhy.

Při zvažování použití VPN je nutné vzít v úvahu celkové měsíční nároky na přenosovou kapacitu i nároky na krátkodobou přenosovou kapacitu ve špičce. Mnoho ISP uplatňuje příplatek, když celkové množství přenesených dat za měsíc překročí určitý objem. Je nepravděpodobné, že by náklady na hodně používané, dlouhodobé připojení k Internetu byly vyšší než náklady na pronájem městské nebo meziměstské linky s podobnou kapacitou, ale přesto je dobré prostudovat nabídky jednotlivých ISP v okolí a podle toho se zařídit.

V souvislosti se zpětným voláním pro vzdálené uživatele má VPN výhodu v tom, že není nutné poskytovat a podporovat vlastní specializované vybavení pro zpětné volání, jako jsou modemy a terminálové servery, ani není potřeba mít k dispozici telefonní linky pro vytáčené připojení. Tuto službu lze svěřit ISP. Náklady na správu a odpisy vybavení by samy o sobě měly ospravedlnit poplatky za uživatelské účty u ISP (a mnoho uživatelů si už doma stejně zařídilo své vlastní účty u ISP).

4.1.2.2 Snadnější implementace VPN

Dva nejzávažnější problémy při výstavbě a správě WAN souvisejí s ustavováním komunikačních propojení přes vyhrazené pronajaté telefonní linky (pomocí specializovaných komunikačních zařízení) a se směrováním provozu WAN přes tyto linky pomocí specializovaných směrovačů. Standardně trvá ustavení tradiční sítě WAN pomocí vyhrazených pronajatých linek nebo Frame Relay minimálně 2 měsíce.

Při ustavování VPN přes Internet pomůže zřídit úvodní připojení IP ke své službě poskytovatel internetových služeb. Jakmile se na firewallu nebo směrovači nastaví vytvoření tunelu, může se směrování svěřit Internetu. Není třeba se učit, jak programovat a spravovat specializované směrovače a brány (pokud se nepoužívají v lokální sítí, jako např. při propojování několika sítí LAN na kampusu). Musí se ale ustavit a spravovat připojení k VPN a také připojení k Internetu .

Každopádně, jakmile se ustaví připojení IP, připojení VPN lze zprovoznit za několik hodin.

4.1.2.3 VPN jsou pomalejší než WAN

Na VPN nelze dosáhnout stejného výkonu jako s počítači, které sdílejí stejnou síť LAN. Standardní přenosové rychlosti na LAN dosahují 10 až 100 Mb/s, ale VPN je kvůli Internetu nejpomalejší z propojení, která připojují zdrojový počítač k cílovému počítači. Když je například počítač se zpětným voláním připojen k Internetu modemem o rychlosti 56 Kb/s, pak bude přenos dat probíhat maximálně rychlostí 56 Kb/s. Pokud se sítě LAN připojují k Internetu přes ISP, který poskytuje pronajaté linky T1, pak lze očekávat maximální přenosovou rychlost pro provoz mezi jednotlivými LAN 1,5 Mb/s (v obou směrech). Samozřejmě sítě WAN jsou stejné. Pokud sítě LAN propojí přímo přes pronajaté linky T, byl by limit přenosové kapacity stejný – 1,5 Mb/s (v obou směrech).

I když je k dispozici velmi rychlé připojení k ISP, není možné využívat celou jeho přenosovou kapacitu, protože mezi lokálním ISP a ISP, který obsluhuje vzdálenou LAN, může být umístěno propojení s nižší rychlostí. K ISP se například připojíte přes FDDI (což je médium s přenosovou rychlostí až 100 Mb/s), ale ISP má třeba k bodu přístupu ke službám, který propojuje ISP, pouze připojení T3, čímž se celková propustnost omezí zhruba na 45 Mb/s. Přenosovou kapacitu Internetu také sdílí ostatní uživatelé Internetu, takže ve skutečnosti lze využívat pouze zlomek maximální teoretické přenosové kapacity.

Navíc síť může závažně zpomalit i dopravní zácpa na Internetu mezi koncovými body VPN. Pokud má VPN mezi svými koncovými body více než 20 mezilehlých systémů, což lze zjistit pomocí příkazu tracert, pravděpodobně bude zbytečně pomalá, obzvlášť pokud těchto 20 systémů vlastní různí ISP. Nejlepší je vyřešit tento problém tím, že se systémy připojí přes jednoho národního nebo mezinárodního ISP. Všechna data pak budou přenášena po jejich privátní síti a síť se vyhne bodům přístupu na síť na ucpaných komerčních internetových ústřednách.

4.1.2.4 VPN jsou méně spolehlivé oproti WAN.

U WAN je k dispozici mnohem větší míra kontroly nad sítí než u VPN. U WAN nastavujete směrovače a brány, domlouváte se na službě přes pronajaté linky pro celou délku trasy mezi jednotlivými sítěmi LAN a nastavujete a spravujete specializovaná zařízení na WAN. Nesdílíte přenosovou kapacitu WAN s žádnou další organizací ani jednotlivci. U VPN se naopak všechna tato rozhodnutí delegují na jedince mimo společnost. Na ustavení první fáze VPN (ze sítě LAN k ISP) spolupracujete vy a ISP, ale všechny ostatní části spravuje někdo jiný. Takže v případě výpadků sítě je k dispozici menší možnost kontroly. Přenosovou kapacitu dostupnou pro uživatele ve VPN mohou také snížit neočekávané výkyvy v činnosti Internetu. Na druhé straně však tito poskytovatelé služeb mají často značné zkušenosti v řešení komunikačních problémů a mohou je opravit mnohem rychleji než běžný administrátor LAN. Pozitivní také je, že přenosová kapacita Internetu neustále roste.

Problém se spolehlivostí se nejúčinněji vyřeší stejně jako problém s rychlostí. V celé síti by se měl použit stejný celostátní ISP. Pokud jsou v síti vzdálení uživatelé pracující z domova, je nutné zajistit, aby ISP také poskytoval komerční služby s vytáčeným připojením, aby tito uživatelé nemuseli při přístupu do sítě směrovat přes komerční internetové ústředny. Odebíráním služeb pouze jediného celostátního ISP se zajistí, že odpovědnost za potíže ponese pouze jediná společnost-nebude nutné se potýkat s tím, že na sebe budou konkurenční společnosti navzájem ukazovat prstem, když se budou chtít vyhnout zodpovědnosti.

4.1.2.5 VPN jsou méně bezpečné než izolované LAN nebo WAN.

Jednou z nevýhod VPN (a nevýhodou, která je asi nejpodstatnější) je, že jsou méně bezpečné než izolované sítě LAN a WAN, které nejsou připojeny k Internetu. Aby mohl hacker napadnout síť, musí najít způsob, jak se na ni dostat. Ale kolik sítí LAN nebo WAN není v dnešní době připojeno k Internetu? VPN je trochu citlivější na průniky do sítě než sítě LAN nebo WAN, které jsou připojeny k Internetu, protože protokol VPN je dalším rozhraním, jež se hacker může pokusit zneužít.

Řešení VPN (např. implementace PPTP od Microsoftu) poskytují hackerům směry útoků, které můžou využít. Všechny metody přístupu do sítě jsou potencionálním směrem útoku a u sítí VPN se směr útoku do sítě vystavuje přímo na veřejném Internetu. Silná opatření ve formě šifrování a autentizace mohou riziko vniknutí téměř úplně vyloučit, ale

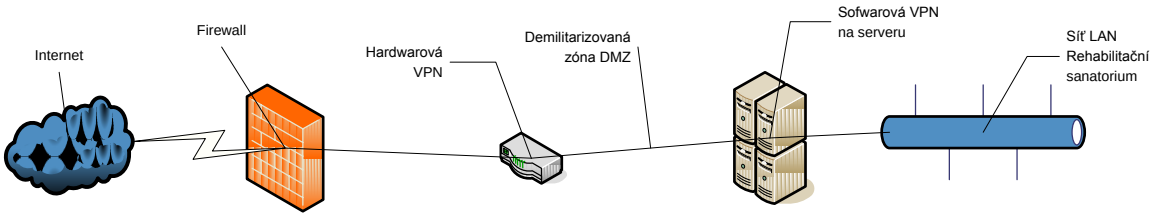
nikdy ho nevyloučí úplně. A veškeré závady v implementaci protokolu VPN výrazně ztíží pozici z hlediska zabezpečení sítě.

4.2 SOFTWAROVÉ ŘEŠENÍ VZDÁLENÉHO PŘÍSTUPU

Základním typem využití sítě VPN je situace, kdy určitý uživatel potřebuje k síti přistupovat z určitého vzdáleného místa. Jestliže se tak například obchodní cestující bude potřebovat dostat k informacím umístěným ve firemní síti, pak mu stačí vytvořit spojení VPN do domovské pobočky, stejně jako kdyby se chtěl připojit z domova do domovské firemní sítě.

Použití virtuální privátní sítě pro vzdálený přístup individuálních uživatelů do firemní sítě, je v konceptu nejjednodušší variantou. Realizaci může ztížit použitý operační systém nebo nainstalované protokoly na straně klienta.

Navrhoval bych na server nahrát softwarové řešení, níže vybrané firmy, které by usnadnilo vzdálený přístup k lokální síti viz obrázek 4.1.2-9.



Obr 4.1.2-9 Řešení vzdáleného přístupu k lokální síti

4.2.1 Softwarové VPN

Softwarově založené VPN pracují na způsobu použití tunelových protokolů. Tuto kategorii je možné dále rozdělit na produkty třetích stran a VPN software, podporovaný operačními systémy. Zřejmou výhodou posledně jmenovaného je cena. Není nutné nic dalšího dokupovat, přičemž řešení virtuální privátní sítě, obsažené například ve Windows 2000, je pro mnoho organizací naprosto dostačující. VPN software třetích stran obvykle obsahují další užitečné vlastnosti, rozšiřují užitečnost VPN, často poskytují více možností zabezpečení a, v

některých případech, snadnější implementaci. Softwarově založené VPN nám umožňují přenášet data založená na protokolu nebo IP adrese. Tento typ filtrování není obvykle u hardwarově založených produktů dostupný.

Produkty třetích stran jsou například Safeguard VPN, Checkpoint SVN (Secure Virtual Networking), Kernun, Cisco a Kerio VPN.

4.2.2 Návrh variant

Softwarové řešení společnosti Check Point Software Technologies

Společnost Check Point Software Technologies je světový lídr v oblasti zabezpečení Internetu. Pevně si drží vedoucí postavení na světovém trhu s VPN a firewally. Architektura Secure Virtual Network (SVN) této společnosti poskytuje VPN a bezpečnostní infrastrukturu, která jedinečným způsobem umožňuje bezpečnou a spolehlivou internetovou komunikaci. SVN řešení, dodávaná ve skupině produktů Next Generation, zabezpečují obchodní komunikaci a zdroje pro podnikové sítě, vzdálené zaměstnance, pobočky a partnerské extranety. Open Platform for Security (OPSEC) společnosti Check Point zvyšuje potenciál SVN řešení tím, že vytváří oborový rámec a alianci za účelem integrace a interoperability nejlepších řešení od více než 300 význačných společností. Řešení firmy Check Point jsou prodávána, integrována a spravována v rámci sítě 2 500 oprávněných partnerů ve 149 zemích.

Softwarové řešení společnosti SafeGuard VPN

SafeGuard VPN nabízí možnost vytvoření virtuální privátní sítě (viz lit. [15]). Pomocí tohoto řešení je možno vytvořit bezpečný přenos dat mezi centrálou a pracovními stanicemi a pro připojení externích nebo cestujících pracovníků.

Přístup virtuální privátní sítě se provádí pomocí standardu X.509 založeným na certifikací. Když se uživatelé připojí k zabezpečené pracovní stanici nebo serveru, v pozadí se objeví osvědčení na základě přihlášení. RSA algoritmus založený na technologii dotaz / odpověď zaručuje, že vetřelec není schopen simulovat falešné přihlašovací údaje. Certifikát zaručuje, že uživatel má k dispozici klíč. Po ověření uživatele, budou všechny údaje mezi uživatelem a serverem šifrovány.

Každý uživatel má veřejný a soukromý klíč. Pro kodifikovaný přenos dat budete potřebovat obojí. Definice úrovně zabezpečení je v tom souboru (Policy), která obsahuje popis balení IP (ESP, AH) a šifrovací algoritmus popisu (Triple-DES 168bit, nebo 128bit IDEA). Tyto algoritmy jsou uznávány jako velmi bezpečné řešení po celém světě.

Platformy

- SafeGuard VPN Gateway: Windows NT 4.0, Windows2000 a novější
- SafeGuard VPN Agent: Windows 95/98, Windows NT 4.0, Windows 2000 a novější
- SafeGuard VPN RAS: Windows NT 4.0, Windows 2000 a novější

Softwarové řešení Kernun

Technologie Kernun VPN Access umožňuje bezpečné propojení geograficky vzdálených počítačových sítí. Tímto propojením vznikne robustní "virtuální privátní síť", v níž uživatelé mohou sdílet všechny dokumenty, databáze, diskový prostor a další zdroje bez ohledu na to, kde jsou tato data fyzicky uložena. Pro koncové uživatele je řešení zcela transparentní a výhodné.[13]

Kernun VPN Access umožňuje i vzdálený bezpečný přístup do interní sítě z jediného počítače, což ocení zejména manažeři či cestující zaměstnanci. Elektronická pošta, databáze, soubory, tiskárny a další zdroje interní sítě vám budou k dispozici odkudkoliv – stačí jen přenosný počítač a připojení k Internetu. O zbytek se postará Kernun VPN Access. [13]

Podporované technologie

Kernun VPN Access podporuje nejrozšířenější protokoly pro vytváření virtuálních privátních sítí – IPSec, OpenVPN (VPN na bázi SSL) a PPTP. Díky tomu se můžete připojit z libovolného operačního systému. [13]

Standardní součásti:

- VPN server: Kernun je velmi flexibilní v možnostech nastavení VPN. Podporované protokoly jsou IPsec/IKE, PPTP, L2TP a OpenVPN; poslední jmenovaný je vhodný jak pro připojení klienta k síti (point-to-multipoint), tak pro propojování sítí (point-to-point); možnosti jeho vlastností přesahují možnosti ostatních protokolů a přitom zůstává jednoduchý a otevřený. Typické nasazení zahrnuje využití X.509 certifikátů a moderní šifrovací metody pro zajištění autenticity, integrity a soukromí. [13]
- Stavová paketová inspekce: Pro řízení spojení lze použít prostředky stavové inspekce. Moderní a velmi pokročilý paketový filtr s možnostmi detekce vzdáleného operačního systému, řízení šířky pásma a ochrany proti DoS útokům poskytuje vysokou bezpečnost i propustnost. Mimo jiného nabízí i obousměrný překlad adres, normalizaci síťového provozu a logování komunikace. [13]

Kerio WinRoute Firewall

Kerio VPN je komplexní řešení, které je snadno použitelné, snadno nastavitelné a transparentní vůči překladu adres (NAT). Řešení firmy Kerio nabízí (viz lit. [14]):

- Propojení sítí — VPN typu server-to-server
- Bezpečné propojení sítě centrály a poboček firmy.
- Bezpečné sdílení síťových zdrojů přes Internet.
- Kerio VPN Client — VPN typu client-to-server

Dále nabízí jednoduchou správu a bezproblémovou konfiguraci. Propojení vzdálených poboček lze nastavit pomocí jednoduchého průvodce. V aplikaci Kerio VPN client stačí zadat jméno nebo IP adresu firewallu (počítače s WinRoute) a uživatelské jméno a heslo. Bezproblémový průchod NAT. VPN tunely server-to-server a client-to-server lze bez problémů vytvářet i v privátních sítích, kde směrovače provádějí překlad IP adres (NAT). Není potřeba speciální podpora pro VPN (tzv. NAT traversal). Kerio VPN používá standardní šifrovací algoritmy: SSL řídicí kanál (TCP) a blowfish pro datový kanál (UDP). Nabízí

flexibilní zabezpečení, kterým lze vzdáleným klientům omezit přístup do lokální sítě komunikačními pravidly firewallu.

Sofwarové řešení společnosti CISCO

Firma Cisco integruje funkce virtuálních privátních sítí VPN přímo do svého hardwaru, na druhé straně ale neopouští ani softwarovou část řešení (viz lit. [12][5]). Jinými slovy, i řešení sítí VPN od firmy Cisco může začínat na vybavení, které nemá vůbec žádné spojení s hardwarem firmy Cisco. Jestliže klientský software Cisco Secure VPN klient nainstalujeme na běžný osobní počítač s MS Windows, pak se může pracovník na dálku, vzdálená kancelář nebo třeba obchodní zástupce na cestách připojit přes libovolnou internetovou síť a vytvořit si svůj vlastní tunel VPN.

Klient může být umístěn na libovolném osobním počítači kdekoliv na světě a cestu k domovskému směrovači nebo PIX firewallu buduje přes běžný, veřejný internet.

Klientský software Cisco VPN client v sobě obsahuje celou řadu funkcí a nástrojů, jejichž úkolem je zajištění bezpečného a stabilního tunelování v protokolu IPSec. Mezi nejdůležitější funkce a vlastnosti patří:

- Síťový administrátor může exportovat a uzamknout bezpečnostní politiku (zásady zabezpečení)
- Klient vyhovuje standardu IPSec, dále podporuje:
    - Zabezpečení v tunelovacím režimu (Tunnel Mode) nebo přenosovém režimu (Transport Mode)
    - Šifrovací algoritmy DES, 3DES, MD-5 a SHA-1
    - Mechanismus výměny klíčů IKE s potvrzováním ISAKMP/Oakley Handshake and Key Agreement.
- Je kompatibilní s většinou komunikačních zařízení Windows, včetně adaptérů sítí LAN, modemů, karet PCMCIA atd.
- Umožňuje pohodlnou centrální konfiguraci.
- Je kompatibilní s certifikačními autoritami podle standardu X.509, jako jsou:
    - Windows 2000 Certificate Services
    - Verisign Onsite
    - Netscape Certificate Management Systém
- Grafické uživatelské rozhraní pro snadnou správu bezpečnostní politiky a certifikátů

- Práce s klientem je transparentní.

4.2.2.1 První kolo výběru nejlepší varianty

Výběr řešení bude dvoukolový. Z prvního kola projdou pouze dvě technologie, které splní nejlépe níže uvedené požadavky, tzn. budou mít nejvíce bodů.

Jelikož se vzdálený přístup k síti ve firmě nevyužívá, proto bude hlavním faktorem pro výběr nejlepší varianty ve druhém kole **cena**.

Stanovená kritéria pro první kolo výběru a jejich váhová hodnota:

- podpora protokolů – váha 4,
- komfort použití systému uživatelem – váha 4
- podpora výrobce –váha 3
- reference na trhu – váha 2.

		Checkpoint SVN		**SafeGuard VPN**		**Kernun**		**Kerio**		**Cisco**	
Kritérium	***Váha***	***Známka***	***Body***	***Známka***	***Body***	***Známka***	***Body***	***Známka***	***Body***	***Známka***	***Body***
Podpora protokolů	4	3	12	3	12	4	16	3	12	3	12
Komfort použití systému uživatelem	4	3	12	3	12	3	12	4	16	3	12
Podpora výrobce	3	2	6	3	9	3	9	3	9	3	9
Reference na trhu	2	3	6	3	6	3	6	3	6	4	8
Celkové bodové hodnocení			**36**		**39**		**43**		**43**		**41**

Tab. 4.2.2.1-1 Tabulka hodnocení variant dle kritérií

Do dalšího kola postoupila řešení firmy Kerio a Kernun. Údaje v tabulce byly konzultovány z IT manažerem.

4.2.2.2 Výběr nejlepší varianty a cenová kalkulace

Kerio WinRoute Firewall – pořizovací cena je 4690 Kč[1] za licenci, která zahrnuje:

- Aplikaci včetně 5 uživatelů (další uživatelé možno dokoupit v blocích po 5 za 442Kč[1]/uživatel.
- Nárok na aktualizaci produktu po dobu 1 rok

[1] Uvedené ceny bez DPH 20%

- Nárok na telefonickou a emailovou technickou podporu po dobu 1 rok
- Nárok na aktualizaci virové databáze McAfee po dobu 1 rok
- Aplikaci Kerio VPN Klient

Obnovení předplatného po 1 roce používání 1410Kč[2] a obnovení uživatelů 134 Kč[2]/uživatel.

Kernun VPN Acces – jelikož se mnou firma Kernun nespolupracovala a po mé prosbě nedodala potřebné informace ohledně cen jejich produktu, nemůžu je tady uvést.

Jako nejlepší variantu řešení vzdáleného přístupu pomocí VPN jsem zvolil řešení společnosti **Kerio.** V kapitole zhodnocení budou přehledně uvedeny náklady na provoz tohoto řešení.

4.3 PŘEDNOSTI A LIMITY VPN U VZDÁLENÉHO PŘÍSTUPU

Technologie VPN je čím dál rozšířenější a své uplatnění nachází v rozličných oblastech. Její přínosy a limity budou popsány níže. (viz lit. [9])

4.3.1 Přínosy a přednosti

Nasazení VPN má mnoho přínosů. Především: VPN dramaticky snižují náklady na spojení. Přestože využití veřejných sítí považujeme za samozřejmost, tak si uvědomme, že právě díky VPN a veřejným sítím nemusíme budovat vlastní nákladné sítě. A to v oblasti, kde by to bylo zhola nemožné. Jen málokterá organizace si může dovolit vybudovat vlastní fyzickou globální síť. Tím se dostáváme k další výhodě, jíž je využití globálních příležitostí, které by jinak pro nás byly nedostupné.

VPN jsou také velmi dobře škálovatelné a má smysl je budovat i kvůli jedinému počítači připojenému z druhého konce světa. Což by pochopitelně bylo v dobách minulých něco naprosto nepředstavitelného.

[2] Uvedené ceny bez DPH 20%

Technologie VPN rozšiřují geografickou konektivitu. Nezáleží na tom, kde a jak jsou rozmístěné jednotlivé počítače či lokální sítě – všechny jsou spolehlivě (a zpravidla bezpečně) propojené.

VPN umožňují v rámci nezabezpečeného spojení předávat data bezpečně a šifrovat data tam, kde by jinak proudila v otevřené podobě. A ještě v jedné oblasti jsou výrazným bezpečnostním přínosem: i vzdálené stanice či servery jsou díky VPN dobře přístupné, takže se administrátorům lépe spravují a bezpečnostní politika na nich se lépe vynucuje. Což by se opět v tradičním prostředí jen obtížně provádělo.

VPN dále výrazně zjednodušují topologii sítě. Pochopitelně, že zde jsou výjimky potvrzující pravidlo, ale v drtivé většině případů je zjednodušení správy a zrychlení provozu takřka „hmatatelné".

V maximální možné míře také VPN umožňují využít stávající hardware a software, tedy dosavadní investice. Při expanzi nebo nasazování nových technologií (např. on-line přístup obchodních cestujících do databáze) není nutné dosavadní investice „oplakat", nýbrž na nich lze stavět.

4.3.2 Limity VPN

Z předešlých řádku jsme mohli nabýt dojmu, že VPN jsou takřka všeřešící, takže je mou povinností upozornit na několik úskalí těchto technologií. Přestože klady VPN převládají, několik háčků na nich přece jen najdeme.

Především je třeba si uvědomit, že musíme velmi kvalitně zajistit bezpečnost na klientské straně. VPN se totiž skládají ze dvou hlavních částí, které můžeme označit jako „vnější" a „vnitřní". V zásadě se dá říci, že proti vnějším hrozbám jsou VPN chráněné dobře (ostatně, byly s tím i navrhované), u vnitřní části je to horší. Jinými slovy: pokud používáme silné šifrování (což je dnes fakticky samozřejmostí), pak vlastní proud dat po veřejné síti (internetu) je chráněný více než solidně. Ovšem běda, pokud se útočník dokáže dostat na některý z přístupových bodů k VPN.

Musíme tedy velmi dbát na fyzickou a administrativní bezpečnost. Je zapotřebí kvalitní „dohled" nad klienty, nad jejich chováním, je nutné vynucovat bezpečnostní politiku. Jinak hrozí, že výhod VPN nebude těžit pouze organizace, ale také nezvaný útočník. (Běžný je např. požadavek, že každý zaměstnanec připojující se z domu musí instalovat hardwarový firewall.)

Z tohoto vyplývají i další omezení: administrátor musí bedlivě sledovat (pochopitelně pomocí vyhodnocovacích nástrojů) veškeré logy z provozu na síti, aby zavčas odhalil pokusy o průnik nebo dokonce vlastní průnik. Ne že by něco podobného nebylo v běžném prostředí nutné dělat, ale v oblasti VPN tato činnost výrazně nabývá na důležitosti.

Každý sebemenší bezpečnostní průnik nebo incident totiž ohrožuje celou síť organizace. A zvláště u velkých VPN sítí je to nepříjemné, protože v globálním světě stačí nepozornost nebo nezkušenost jednoho zaměstnance na jiném světadíle – a v ústředí společnosti mohou nastat nemalé problémy.

Zde je potřeba si také uvědomit nutnost správného vybudování celé architektury sítě, protože data předávaná pomocí VPN jsou pro ostatní prvky „neviditelná“ (nečitelná – díky šifrování).

Byť VPN v konečném důsledku zvyšuje bezpečnost při komunikaci pomocí internetu nebo jiné nedůvěryhodné sítě, tak se při špatném navržení architektury může stát ohrožením pro bezpečnost sítě lokální.

Každopádně: virtuální privátní sítě jsou velmi kvalitním nástrojem pro omezení rizik plynoucí z geografické roztříštěnosti informačních technologií – včetně mobility jednotlivých zařízení.

4.4 SOFTWAROVÉ VS. HARDWAROVÉ ŘEŠENÍ

Obecně nelze říci, které z těchto řešení je lepší (viz lit. [6], [8]). Každá síť má své vlastní specifické požadavky. V následujícím textu budou popsány výhody, nevýhody a vlastnosti obou řešení.

Softwarové řešení vyniká nízkou cenou, obzvláště když základní software je již obsažen v operačním systému. Například stanice s OS Windows mají nezbytný software pro použití VPN Windows serveru.

Avšak existuje řada silných argumentů proti používaní softwarového (SW) řešení VPN. Hlavním z nich je bezpečnost. Na serveru může běžet, a většinou také běží, spousta aplikací. Pokud se operační systém či kterákoliv aplikace stane zranitelnou, tak je zranitelný celý systém. Z toho vyplývá, že pokud kompromitujeme systém, můžeme tak kompromitovat i VPN službu a opačně. Nebezpečný SW, jakým jsou například viry a tzv. červi, mnohem více ohrožují Softwarová řešení oproti Hardwarovým.

Autentizace a šifrování ve VPN může také hrát významnou roli v zatížení serveru určeného pro všeobecné účely. SW varianta je spíše vhodnější pro situaci, kdy VPN občas

využívá několik uživatelů. V jiných případech je vhodnější zvolit pro realizaci VPN specializované HW zařízení. HW řešení také vyniká nad SW v rychlosti a umožňuje větší počet současně běžících VPN spojení.

5 ZHODNOCENÍ PŘÍNOSU NAVRHOVANÉHO ŘEŠENÍ

Poslední kapitolou je zhodnocení navrhovaného řešení. Provedu zhodnocení jednak kvalitativní, kde se pokusím o identifikaci nejvýraznějších přínosů racionalizace a jednak zhodnocení kvantitativní, kde porovnám náklady řešení s náklady stávajícího stavu, který by mohl být nahrazen navrženou racionalizaci.

5.1 ZHODNOCENÍ PŘÍNOSU ZMĚNY PRONAJATÉ LINKY NA VPN SPOJENÍ

5.1.1 Kvantitativní zhodnocení

Tato podkapitola zobrazuje peněžní vyjádření přínosů projektu. Doba jednotky produkčního cyklu systému je stanovena na 2 roky. Předpokládaný produkční cyklus VPN je stanoven na 2 jednotky cyklu, tedy 4 roky. Cenové kalkulace jsou tedy vztaženy k této době.

Poznámka 1: Všechny ceny uvedené bez DPH 20%.

VPN:

Celková pořizovací cena HW:	22 000,- Kč
Roční provozní náklady:	72 000,- Kč
Jednorázový poplatek zavedení Internetu:	3 000,- Kč
Celkové náklady za 4 roky:	313 000,- Kč

WAN(pronajatá linka)

Roční provozní náklady:	180 000,- Kč
Celkové náklady za 4 roky:	720 000,- Kč

Rozdíl mezi WAN a VPN za 4 roky: 407 000,- Kč

Ze zobrazených nákladů vychází, že propojení poboček virtuální privátní sítí je levnější oproti pronajaté linky, a rozdíl v nákladech za čtyřleté období činí 407 000,- Kč (což by mohlo odpovídat dalšímu více jak 5 letému provozování VPN). Toto je hlavní přínos racionalizované sítě.

Dále spočítám dobu návratnosti investice do VPN propojení poboček a sítí WAN s pronajatou linkou., tedy dobu, za jak dlouho se vrátí finanční prostředky vložené do racionalizace propojení pracovišť.

Doba návratnosti investice, vzorec $t_n = I/\Delta Z$

kde t_n=doba návratnosti
I= investice (v Kč)
ΔZ= efekt (v Kč) – rozdíl mezi náklady

tedy

t_n= 25 000/(180 000-72 000)
t_n=25 0000/108 000
t_n=0,231 roku

Doba návratnosti investice do propojení pomocí VPN je proti provozu s pronajatou linkou **3 měsíce**.

5.1.2 Kvalitativní zhodnocení

Dobré kvalitativní zhodnocení a dosažení stejné úrovně spolehlivosti a rychlosti je pro Lázně Darkov stejně důležité jako samotná úspora. Tato změna sebou přinese:

- Snadnější implementaci
- Stejnou rychlost připojení
- Spolehlivé připojení
- Celková hospodárnost ve větším měřítku (Internetové služby jsou podstatně méně nákladné než interní, vnitropodnikové týmy, specializované na sítě WAN).

5.2 ZHODNOCENÍ PŘÍNOSU VZDÁLENÉHO PŘÍSTUPU POMOCÍ VPN

5.2.1 Kvantitativní zhodnocení

Jelikož se ve Lázních Darkov nepoužívala žádná možnost vzdáleného přístupu, je těžko ho hodnotit kvantitativně, protože ho nemáme s čím porovnávat, proto se budu věnovat jen kvalitativnímu hodnocení. V této kapitole uvedu pouze náklady na provoz.

Poznámka 1: Všechny ceny uvedené bez DPH 20%.

SW VPN

Náklady na pořízení:	4690,-Kč (5 uživatelů) + 4420,-Kč (10 uživatelů)
Roční náklady na provoz:	1410,-Kč (prodloužení licence) + 2010,-Kč (15 uživatelů)
Celkové náklady za 4 roky:	19 370,-Kč (15 uživatelů)

5.2.2 Kvalitativní zhodnocení

Mezi kvalitativní aspekty hodnocení vzdáleného přístupu pomocí VPN jsou:

- Mobilita pracovníků.
- Komfortní použití a větší mobilita uživatele k místu připojení.
- Možnost práce s pomalým i rychlým připojením k Internetu z domova.
- Zvýšení bezpečnosti na úrovní uživatele (pokročilé funkce ověřování atd.).
- Komfortní administrace – snadná a rychlá správa.
- Vysoká dostupnost a redundance.
- Možnost přístupu k interním zdrojům firmy a velká škálovatelnost nastavení přístupu.

6 ZÁVĚR

V této diplomové práci jsem se zabýval možností využití virtuálních privátních sítí v akciové společnosti Lázně Darkov. V úvodní části jsem se zaměřil na vymezení motivace a důvody budování virtuálních privátních sítí a vliv rozvoje Internetu na tento typ připojení.

Druhá kapitola diplomové práce tvoří její teoretickou část. Jsou v ní popsány základní rozdíly mezi sítěmi LAN a WAN a dále je vysvětlena technologie VPN, která je v dnešní době stále žádanější. Čtenář by tak měl získat dostatek informací, aby byl obeznámen s tím, jak tato technologie funguje. V rámci této kapitoly je vysvětlen pojem virtuální privátní síť dále pak typy VPN, architektury VPN, typologie VPN, běžné implementace VPN, kde jsou popsány nejznámější protokoly, na kterých VPN funguje. Dále je pak popsáno fungování bezpečného vzdáleného přístupu.

V další kapitole jsem stručně popsal objekt řešení, tj. Lázně Darkov jejich historii a jejich dvě léčebná zařízení a dále jsem analyzoval jejich počítačovou síť, její topologii a použitý harware pro zjištění, zda se ve firmě dá využít virtuální privátní sítě.

Ve čtvrté kapitole jsem se věnoval návrhu možného využití VPN jak v možnosti propojení Rehabilitačního sanatoria a Léčebny Darkov tak i možného přístupu vzdálených individuálních pracovníků k podnikové síti a dále vybral podle mého názoru nejlepší řešení pro hardwarové propojení pracovišť a softwarové řešení vzdáleného přístupu a uvedl jejich kalkulace.

Poslední kapitola je věnována zhodnocení přínosu navrhovaného řešení pomocí VPN namísto stávajícího řešení, což je v propojení dvou pracovišť síť WAN s pronajatou linkou a dále přínosy VPN ve vztahu k vzdálenému přístupu k podnikové síti.

Na závěr lze říci, že cíl této práce byl splněn a může tedy být využita jako podklad pro rozhodnutí oddělení informatiky, zda se rozhodnout pro využívání virtuálních privátních sítí v řešeném podniku Lázně Darkov, a.s.

SEZNAM POUŽITÉ LITERATURY

Knihy

1) OSTERLOH, Heather. *TCP/IP : Kompletní průvodce*. Praha : SoftPress, 2003. 512 s. ISBN 80-86497-34-8.

2) PETERKA, Jiří. *Co je čím ... v počítačových sítích*. Praha. 237 s. Oborová práce. Matematicko-fyzikální fakulta UK.

3) STREBE, Matthew; PERKINS, Charles. *Firewally a proxy servery : Praktický průvodce*. Vydání první. Brno : Computer Press, 2003. 450 s. ISBN 80-7226-983-6.

4) TRULOVE, James. *Sítě LAN : Hardware, instalace, zapojení*. Tomáš Znamenáček. 1. vyd. Brno : Grada Publishing, 2009. 384 s. ISBN 978-80-247-2098-2.

5) VELTE, Toby J.; VELTE, Anthony T. *Síťové technologie CISCO : Velký průvodce*. Vydání první. Brno : Computer Press, 2003. 759 s. ISBN 80-7226-857-0.

6) WILLIAMS, Andrew. *Firewall policies and VPN Configurations*. Canada : Syngress Publishing, 2006. 482 s. ISBN 1-59749-088-1.

Internetové odkazy

7) LUHOVÝ, Karel. Virtuální privátní sítě VPN. *Svět sítí* [online]. 6. ledna 2003, 6, [cit. 2010-03-10]. Dostupný z WWW: <www.svetsiti.cz>.

8) PLOTNICK, Neil. *Software vs hardware VPN* [online]. c2007 [cit. 2010-03-16]. Dostupný z WWW:<http://vpn.sockslist.net/>

9) PŘIBYL, Tomáš. Virtuální privátní sítě pro vzdálený přístup. *ICT Security* [online]. 17. března 2010, 16, [cit. 2010-03-14]. Dostupný z WWW: <http://www.ictsecurity.cz/>.

10) Připojení do firmy – bez VPN ani byte. *Connect : Nejlepší časopis pro IT profesionály* [online]. 11.1. 2006, 01-2006, [cit. 2010-03-14]. Dostupný z WWW: <http://connect.zive.cz>.

11) KERST, Undo. VPN: vzdálený přístup bez kompromisů. *Security World* [online]. 2008, 4, [cit. 2010-04-14]. Dostupný z WWW: <http://securityworld.cz/securityworld/VPN-vzdaleny-pristup-bez-kompromisu-1-1771>.

12) *Cisco* [online]. 1992-2010 [cit. 2010-04-14]. Cisco Systems, Inc. Dostupné z WWW: <http://www.cisco.com/>.

13) Trusted Network Solutions, a.s. [online].
Dostupný z WWW: http://www.kernun.cz/technologie-kernun/kernun-vpn-access

14) Kerio[online]. Dostupný z WWW: http://www.kerio.cz/cz/firewall/vpn

15) SafeGuard VPN [online]. Dostupný z WWW: http://www.ediport.hu/_sgvpn.html

16) http://www.wikipedia.org

17) Lázně Darkov, a.s. [online]. Dostupný z WWW: http://www.darkov.cz

SEZNAM ZKRATEK A SYMBOLŮ

AH	Authentication Header
ATM	Asynchronous Transfer Mode
CIR	Committed Information Rate
CLP	Cell Loss Priority
DE	Discard Eligible
DSL	Digital Subscriber Line
ESP	Encapsulating Security Payload
FTP	File Transfer Protocol
Gbps	Gigabit za sekundu
GRE	Generic Routing Encapsulation
HTTP	Hypertext Transfer Protocol
IKE	Internet Key Exchange
IP	Internet Protocol
IPSec	IP Security
ISDN	Integrated Services Digital Network (Digitální síť integrovaných služeb)
ISP	Internet Service Provider
Kč	korun českých
LAN	Local Area Network
L2F	Layer 2 Forwarding
L2TP	Layer 2 Tunneling Protocol
NAT	Network Adress Translation
NNTP	Network News Transfer Protocol
PoPToP	PPTP Server pro Linux
PPP	Point-to-Point Protocol
PPTP	Point-to-Point Tunelling Protocol
RRAS	Routing and Remote Access
SA	Security Association
SMTP	Simple Mail Transfer Protocol
SSH	Secure Shell
SSL	Secure Sockets Layer
TCP/IP	Transmission Control Protocol/Internet Protocol
VPN	Virtual Private Network
WAN	Wide Area Network
t_n	doba návratnosti investice

PROHLÁŠENÍ O VYUŽITÍ VÝSLEDKŮ DIPLOMOVÉ PRÁCE

Prohlašuji, že

- jsem byl seznámen s tím, že na mou diplomovou práci se plně vztahuje zákon č. 121/2000 Sb. – autorský zákon, zejména § 35 – užití díla v rámci občanských a náboženských obřadů, v rámci školních představení a užití díla školního a § 60 – školní dílo;

- beru na vědomí, že Vysoká škola báňská – Technická univerzita Ostrava (dále jen VŠB-TUO) má právo nevýdělečně ke své vnitřní potřebě diplomovou práci užít (§ 35 odst. 3);

- souhlasím s tím, že diplomová práce bude v elektronické podobě archivována v Ústřední knihovně VŠB-TUO a jeden výtisk bude uložen u vedoucího diplomové práce. Souhlasím s tím, že bibliografické údaje o diplomové práci budou zveřejněny v informačním systému VŠB-TUO;

- bylo sjednáno, že s VŠB-TUO, v případě zájmu z její strany, uzavřu licenční smlouvu s oprávněním užít dílo v rozsahu § 12 odst. 4 autorského zákona;

- bylo sjednáno, že užít své dílo – diplomovou práci nebo poskytnout licenci k jejímu využití mohu jen se souhlasem VŠB-TUO, která je oprávněna v takovém případě ode mne požadovat přiměřený příspěvek na úhradu nákladů, které byly VŠB-TUO na vytvoření díla vynaloženy (až do jejich skutečné výše).

V Ostravě dne ……..

……..
jméno a příjmení studenta

Adresa trvalého pobytu studenta:

……